

SUSE LINUX

Guide de l’administrateur

Édition 3 2005

Pour toute remarque ou commentaire, veuillez contacter `mailto:documentation@suse.de`.

Auteurs:	Stefan Behlert, Frank Bodammer, Stefan Dirsch, Olaf Donjak, Roman Drahtmüller, Torsten Duwe, Thorsten Dubiel, Thomas Fehr, Stefan Fent, Werner Fink, Kurt Garloff, Carsten Groß, Joachim Gleißner, Andreas Grünbacher, Franz Hassels, Andreas Jaeger, Klaus Kämpf, Hubert Mantel, Lars Marowsky-Bree, Johannes Meixner, Lars Müller, Matthias Nagorni, Anas Nashif, Siegfried Olschner, Peter Pöml, Thomas Renninger, Heiko Rommel, Marcus Schäfer, Nicolaus Schüler, Klaus Singvogel, Hendrik Vogelsang, Klaus G. Wagner, Rebecca Walter, Christian Zoz
Traduction:	Patricia Vaz
Rédaction:	Jörg Arndt, Antje Faber, Karl Eichwalder, Berthold Gunreben, Roland Haidl, Jana Jaeger, Edith Parzefall, Ines Pozo, Thomas Rölz, Thomas Schraitle
Mis en page:	Manuela Piotrowski, Thomas Schraitle
Typographie:	DocBook-XML, LaTeX

Ce livre a été imprimé sur papier blanchi sans aucune addition de chlore.

Bienvenue

Félicitations pour votre nouveau système d'exploitation LINUX et merci beaucoup d'avoir choisi SUSE LINUX 9.3. L'achat de cette version vous donne droit à l'assistance technique à l'installation par téléphone et courrier électronique comme décrit à l'adresse `http://www.novell.com/products/linuxprofessional/support/conditions.html`. Pour bénéficier de ce service, activez votre droit à l'assistance sur le portail de SUSE LINUX (`http://portal.suse.com`) à l'aide du code imprimé sur l'emballage de vos CD-ROM.

Afin que votre système soit toujours en sécurité et à jour, nous vous conseillons de le mettre à jour régulièrement avec le confortable YaST Online Update. De plus, SUSE vous propose une lettre d'information électronique gratuite présentant des informations relatives à la sécurité et des trucs et astuces pour SUSE LINUX. Il vous suffit de vous inscrire en saisissant votre adresse de courrier électronique à l'adresse `http://www.novell.com/company/subscribe/`.

Le *Guide de l'administrateur* SUSE LINUX vous apporte des informations générales sur le fonctionnement de votre système SUSE LINUX. Ce manuel vous initiera aux bases de l'administration système sous Linux, comme les systèmes de fichiers, les processus d'amorçage et la configuration du serveur web Apache. Le *Guide de l'administrateur* SUSE LINUX se compose de cinq parties principales :

Installation L'installation et la configuration d'un système avec YaST, les variantes d'installation spéciales, le gestionnaire de volumes logiques (LVM), la configuration du RAID, les mises à jour et la réparation du système.

Système Les caractéristiques principales de SUSE LINUX, des détails sur le noyau, à l'amorçage et au processus d'initialisation, à la configuration du gestionnaire d'amorçage et du système X Window, à l'utilisation d'une imprimante et au travail nomade sous Linux.

Services L'intégration dans des réseaux hétérogènes, la configuration du serveur web Apache, la synchronisation des fichiers et la sécurité.

Administration Les listes de contrôle d'accès (ACL) et les outils de surveillance du système importants.

Annexes Sources d'information importantes relatives à Linux.

Vous trouverez les versions numériques des manuels SUSE LINUX dans le répertoire `/usr/share/doc/manual/`.

Nouveautés dans le manuel de l'administrateur

Voici les modifications qui ont été apportées à la version précédente de ce manuel (SUSE LINUX 9.2) :

- Les sections LVM et partitionnement ont été revues. Voyez la section 3.7 page 104 et la section 2.7.5 page 75.
- Le chapitre 8 page 183 a été révisé et une description du module de YaST a été ajoutée. Il contient également une nouvelle section sur l'utilisation des caractères joker. Voyez la section Utilisation de caractères joker pour sélectionner le noyau d'amorçage page 192.
- Le chapitre relatif au système de fichiers s'est enrichi d'une nouvelle section consacrée au système de fichiers Reiser4. Voyez la section 20.2.5 page 395.
- La partie consacrée au réseau a été complètement revue et restructurée. Voyez la partie **??** page ??.
- SuSEfirewall2 a été mis à jour et une description du nouveau module YaST a été ajoutée. Voyez la section Configuration avec YaST page 635.
- Plusieurs nouveaux programmes sont mentionnés dans le chapitre 36 page 677.
- Le glossaire a été revu et actualisé. Voyez le glossary V page 729.

Conventions typographiques

Ce livre utilise les conventions typographiques suivantes :

- `/etc/passwd` : des noms de fichier ou de répertoire
- ⟨*joker*⟩ : le symbole ⟨*joker*⟩ est à remplacer par sa valeur réelle
- `PATH` : une variable d'environnement nommée PATH

- `ls` : une commande
- `--help` : des options et paramètres
- `utilisateur` : un utilisateur
- Alt : une touche sur laquelle il faut appuyer
- 'Fichier' : des éléments de menu, des boutons
- Processus tué : des messages du système
- man man(1) : référence à des pages de manuel
- ► **x86, AMD64**
  Cette section ne concerne que les architectures spécifiées. Les flèches marquent le début et la fin du bloc de texte. ◄

Remerciements

Les développeurs de Linux font avancer Linux dans le cadre d'une collaboration mondiale axée sur le bénévolat. Nous les remercions pour leur engagement — cette distribution n'aurait pu voir le jour sans eux. Nous souhaitons aussi tout spécialement remercier Frank Zappa et Pawar. Et bien entendu nous remercions particulièrement Linus Torvalds.

Have a lot of fun !

Votre équipe SUSE

Table des matières

Première partie

Installation

Installation avec YaST

Ce chapitre vous guide méthodiquement pendant que vous installez le système SUSE LINUX avec YaST, l'assistant du système. Vous apprendrez comment préparer la procédure d'installation et vous obtiendrez des informations de base qui vous aideront à prendre les bonnes décisions lors des différentes étapes de la configuration.

1.1 Amorçage du système pour l'installation

Insérez le premier CD-ROM ou le DVD de SUSE LINUX dans le lecteur et redémarrez votre machine. Le programme d'installation de SUSE LINUX se lancera alors depuis le support dans le lecteur.

1.1.1 Options d'amorçage

Certaines options d'amorçage permettent d'amorcer autrement que depuis un CD ou un DVD. On peut les utiliser lorsque l'on éprouve des difficultés à amorcer depuis un CD ou un DVD. Ces options sont décrites dans le tableau 1.1 de la présente page.

TAB. *1.1: Options d'amorçage*

Option d'amorçage	**Application**
CD-ROM	C'est la possibilité d'amorçage la plus simple. Dans ce cas, le système a besoin d'un lecteur de CD-ROM local pris en charge par Linux.
Disquette	Vous trouverez sur le premier CD, dans le répertoire `/boot/`, les images nécessaires pour créer des disquettes d'amorçage. Consultez le fichier `README` dans ce même répertoire.
PXE ou BOOTP	Cela doit être pris en charge par le BIOS ou par le micrologiciel (firmware) du système utilisé et un serveur d'amorçage doit être disponible dans le réseau. Un autre système SUSE LINUX peut également assurer cette fonction.
Disque dur	SUSE LINUX peut également amorcer depuis le disque dur. À cette fin, vous copiez sur le disque dur le noyau (`linux`) et le système d'installation (`initrd`) depuis le répertoire `/boot/loader` du premier CD et ajoutez le choix correspondant dans le chargeur d'amorçage.

1.1.2 Problèmes éventuels lors de l'amorçage

Des problèmes peuvent apparaître lors de l'amorçage depuis le lecteur de CD ou de DVD si vous avez un matériel trop ancien ou non pris en charge. Votre lecteur de CD ROM peut ne pas être en mesure de lire l'image d'amorçage (boot image) du premier CD. Dans ce cas, utilisez le CD 2 pour amorcer le système. Le CD 2 contient une image d'amorçage conventionnelle de 2,88 Mo que même les lecteurs non pris en charge peuvent lire, et qui vous permet de réaliser l'installation par le réseau.

La séquence d'amorçage de l'ordinateur peut ne pas être configurée correctement dans le BIOS (Basic Input Output System). Vous trouverez les instructions pour modifier la configuration du BIOS dans la documentation de votre carte mère. Des instructions de bases sont données dans les prochains paragraphes.

Le BIOS est le programme permettant d'utiliser les fonctions de base de l'ordinateur. Les constructeurs de cartes mères mettent à votre disposition un BIOS spécialement adapté à votre système. Normalement, on ne peut accéder au paramétrage du BIOS qu'à un moment bien précis lors de l'amorçage. Durant cette phase d'initialisation, la machine réalise un certain nombre de tests de diagnostic matériel. L'un de ces tests est le contrôle de la mémoire, indiqué par un compteur de mémoire. Lorsque ce compteur apparaît, cherchez une ligne, située sous le compteur ou dans la partie inférieure de l'écran : cette ligne indique sur quel touche appuyer pour entrer dans le paramétrage du BIOS. En général, les touches à utiliser sont Suppr, F1 ou Échap. Appuyez sur la touche correspondante jusqu'à ce que l'écran de paramétrage du BIOS apparaisse.

Important

Disposition du clavier dans le BIOS

La configuration du BIOS repose fréquemment sur une disposition américaine du clavier.

Important

Une fois le paramétrage du BIOS démarré, modifiez la séquence d'amorçage comme suit : s'il s'agit d'un AWARD BIOS, cherchez le choix 'BIOS FEATURES SETUP'. D'autres constructeurs emploient des noms semblables comme, par exemple, 'ADVANCED CMOS SETUP'. Choisissez la proposition correspondante et confirmez en appuyant sur Entrée.

Dans l'écran qui apparaît, recherchez la sous-option 'BOOT SEQUENCE'. La séquence d'amorçage par défaut est souvent 'C, A' ou 'A, C'. Dans le premier cas, lors de l'amorçage, l'ordinateur recherche tout d'abord un support amorçable

sur le disque dur (C) et ensuite dans le lecteur de disquettes (A). Appuyez sur la touche (Page précédente) ou (Page suivante) aussi longtemps que nécessaire pour voir apparaître la séquence 'A,CDROM,C'.

Quittez la configuration du BIOS en appuyant sur la touche (Échap). Sélectionnez 'SAVE & EXIT SETUP' ou appuyez sur la touche (F10) pour enregistrer vos modifications. Confirmez vos modifications en appuyant sur la touche (Y).

Si vous possédez un lecteur de CD-ROM SCSI, changez le paramétrage du BIOS SCSI.Dans le cas d'un contrôleur hôte Adaptec, par exemple, vous accédez au paramétrage du BIOS par la combinaison de touches (Ctrl)-(A). Choisissez ensuite 'Disk Utilities' qui affiche la liste des composants matériels connectés. Notez l'identifiant SCSI (SCSI ID) de votre lecteur de CD ROM. Quittez le menu en appuyant sur la touche (Échap) et ouvrez ensuite 'Configure Adapter Settings'. Dans 'Additional Options', choisissez 'Boot Device Options' et appuyez sur la touche (Entrée). Saisissez l'identifiant de votre lecteur de CD-ROM et appuyez encore une fois sur la touche (Entrée). Appuyez alors deux fois sur la touche (Esc) pour revenir au revenir à l'écran de démarrage du BIOS SCSI. Quittez cet écran après avoir confirmé avec 'Yes' le réamorçage de l'ordinateur : boot .

1.2 L'écran d'accueil

L'écran d'accueil affiche différentes options de la procédure d'installation. L'option 'Boot from Hard Disk' démarre le système déjà installé. Cette option est l'option par défaut, car le CD reste souvent dans le lecteur à la fin de l'installation. Pour installer le système, choisissez une des options d'installation à l'aide des touches de direction (flèches). Les différentes options sont :

Installation Le mode d'installation normal dans lequel toutes les fonctionnalités modernes du matériel sont activées.

Installation—ACPI désactivé Si l'installation normale échoue, cela peut être dû à ce que le matériel ne prend pas en charge l'ACPI (Advanced Configuration and Power Interface). Si cela vous semble être le cas, vous pouvez utiliser cette option pour procéder à une installation sans prise en charge de l'ACPI.

Installation—Mode sûr Amorce le système en désactivant le mode DMA (pour les lecteurs de CD-ROM) et les fonctionnalités de gestion d'énergie. Les experts peuvent également utiliser la ligne de commande pour saisir ou modifier des paramètres du noyau.

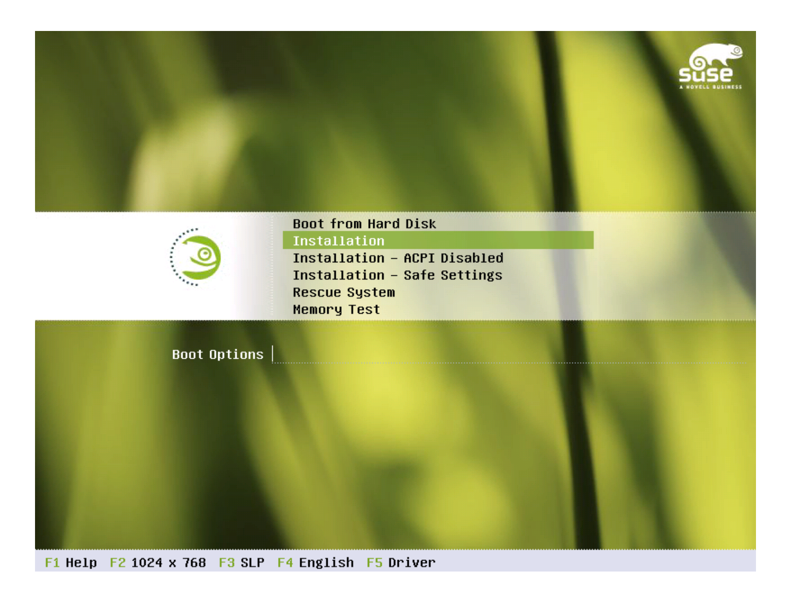


FIG. 1.1: *L'écran d'accueil*

Utilisez les touches de fonctions mentionnées en bas de l'écran pour modifier un certain nombre de réglages d'installation.

- **F1** Vous obtenez une aide contextuelle relative à l'élément activé de l'écran de démarrage.
- **F2** Choix parmi différents modes graphiques pour l'installation. Si des problèmes surviennent lors de l'installation graphique, vous pouvez choisir ici le mode texte.
- **F3** Normalement, l'installation se fait depuis le support de données inséré. Vous pouvez choisir ici d'autres sources d'installation telles que, par exemple, FTP ou NFS. Lorsque l'on installe en réseau avec un serveur SLP, l'une des sources d'installation disponibles sur ce serveur peut être choisie avec cette option. Vous trouverez plus d'informations relatives à SLP dans le chapitre 23 page 459.
- **F4** Vous pouvez ici définir la langue pour l'écran de démarrage.
- **F5** Utilisez cette option pour informer le système que vous disposez d'une disquette de mise à jour des pilotes pour SUSE LINUX. Il vous sera demandé

d'insérer la disquette de mise à jour au moment adéquat de la procédure d'installation.

Lors de l'installation, quelques secondes après l'écran de démarrage, SUSE LINUX charge un système Linux minimal qui contrôlera la suite de la procédure d'installation. Si vous avez choisi les modes d'affichage 'Native' ou 'Verbose', l'écran affiche maintenant de nombreux messages et mentions de copyright. Le programme YaST est lancé à la fin du processus de chargement. Quelques secondes plus tard, vous voyez apparaître l'interface graphique.

C'est maintenant que commence l'installation proprement dite de SUSE LINUX. Tous les écrans de YaST sont disposés de la même manière. Vous avez accès à tous les boutons, à tous les champs de saisie et à toutes les listes de sélection à la fois avec la souris et au clavier. Si le pointeur de la souris ne bouge pas, cela signifie que votre souris n'a pas été reconnue automatiquement. Utilisez dans ce cas le clavier pour l'instant. La navigation au clavier ressemble à celle qui est décrite dans la section 2.9.1 page 85

1.3 Choix de la langue

YaST, et d'une manière générale SUSE LINUX, peuvent être configurés pour utiliser des langues différentes selon vos besoins. La langue que vous choisirez ici s'appliquera servira aussi à déterminer la disposition du clavier. En outre, YaST essaye de deviner le fuseau horaire de l'heure système en fonction de la langue que vous avez choisie. Vous pouvez modifier ces paramètres plus tard en même temps que vous procéderez à la selection des langues secondaires à installer sur votre système. Si votre souris ne fonctionne pas, déplacez-vous à l'aide des touches de direction (flèches) jusqu'à la langue que vous désirez puis appuyez sur la touche Tab aussi longtemps qu'il sera nécessaire pour que le bouton 'Suivant' soit activé. Appuyez ensuite sur la touche Entrée pour confirmer votre choix de langue.

1.4 Mode d'installation

Choisissez 'Nouvelle Installation' ou 'Mise à jour d'un système déjà existant'. On ne peut mettre à jour que si une version de SUSE LINUX est déjà installée sur votre machine. Dans ce cas, vous pouvez aussi décider de démarrer le système

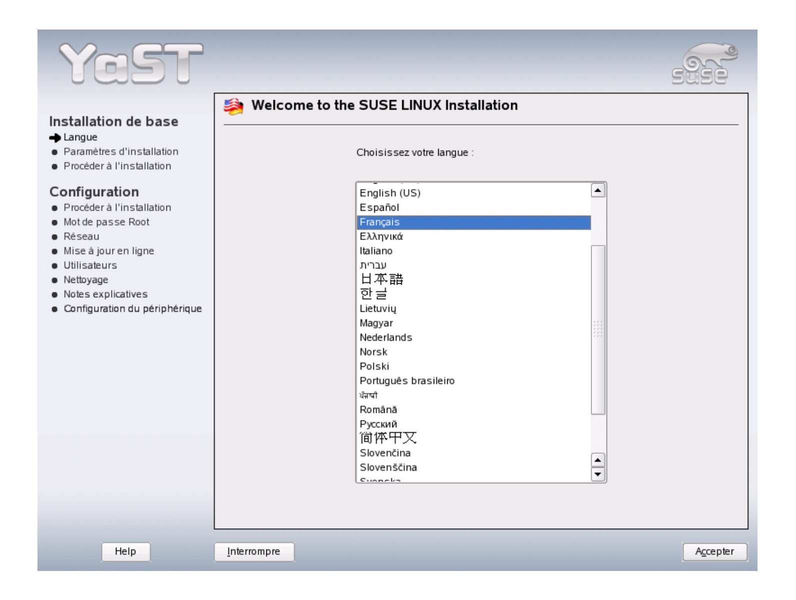


FIG. 1.2: *Choisir la langue*

installé avec 'Démarrer le système installé'. Si votre système installé ne démarre pas, au cas où, par exemple, d'importants paramètres de configuration du système ont été endommagés, vous pouvez utiliser l'option 'Réparation du système installé' pour tenter de rendre le système à nouveau amorçable. Si vous n'avez pas encore installé de système SUSE LINUX, vous ne pourrez procéder qu'à une nouvelle installation. Reportez-vous à la figure 1.3 page suivante.

Les sections qui suivent décrivent la procédure d'installation d'un nouveau système. Vous pourrez trouver des informations détaillées sur la mise à jour du système dans la section 2.2.5 page 52. Vous trouverez une description des possibilités de réparation du système dans le chapitre 5 page 149.

1.5 Suggestions d'installation

À la fin du processus de détection du matériel, vous voyez s'afficher dans la page de suggestions (voir la figure 1.4 page 11) des informations sur le matériel détecté

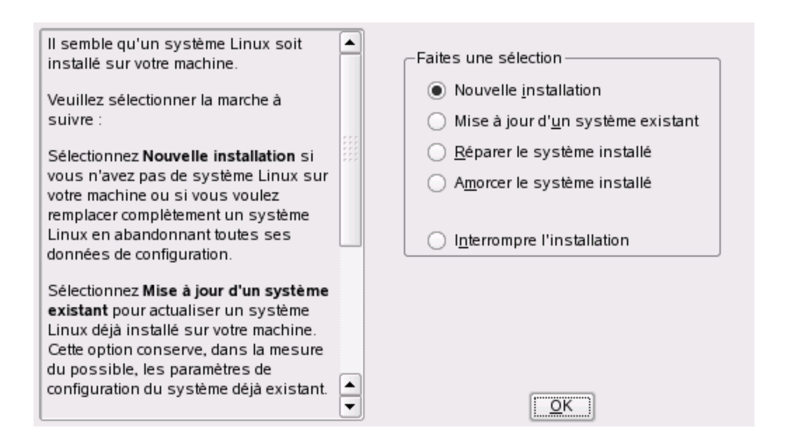


FIG. 1.3: *Choix du mode d'installation*

ainsi que des suggestions pour l'installation et le partitionnement. Si vous cliquez sur une option et effectuez ensuite une configuration, vous reviendrez toujours à cette page qui affichera les suggestions ainsi que les valeurs qui ont été modifiées. Les réglages que vous pouvez effectuer pour la configuration vont être décrits dans les sections suivantes.

1.5.1 Mode d'installation

Ici, vous avez encore la possibilité de changer le mode d'installation choisi auparavant. Les choix possibles sont les mêmes que ceux décrits dans la section 1.4 page 8.

1.5.2 Disposition du clavier

Choisissez la disposition du clavier que vous désirez utiliser. Elle correspond par défaut à la langue que vous avez choisie. Tapez ensuite (Y) et (Z) ainsi que des caractères accentués pour vérifier que votre choix est correct. Cliquez sur 'Suivant' pour revenir à la page de propositions.

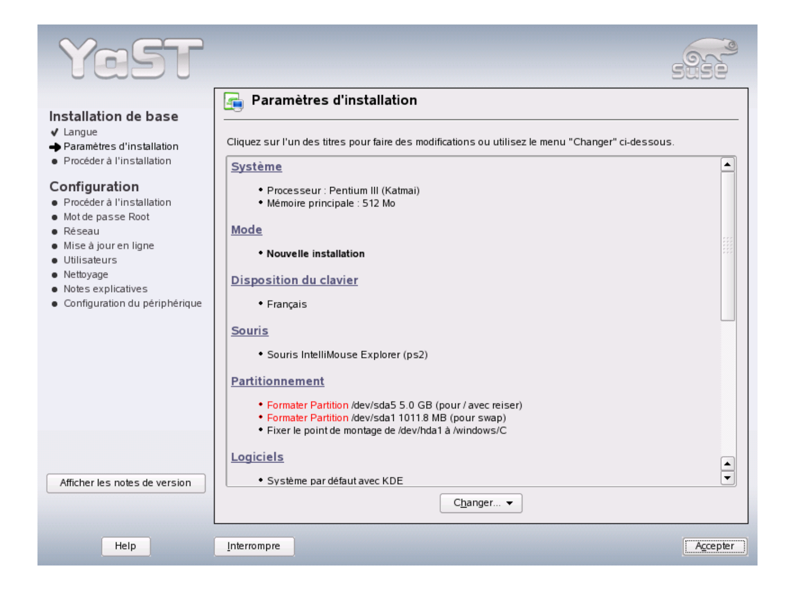


FIG. 1.4: *La page de suggestions*

1.5.3 Souris

Si YaST n'a pas détecté automatiquement la souris, déplacez-vous tout d'abord à l'aide de la touche (Tab) jusqu'à ce que l'option 'Souris' soit sélectionnée. Avec la touche d'espacement, vous obtiendrez l'affichage du formulaire de sélection du type de souris qui vous est présenté dans la figure 1.5 page suivante.

Choisissez le type de la souris à l'aide des touches (↑) et (↓). Consultez la documentation fournie avec votre souris pour en connaître le type. Une fois que vous avez choisi un type de souris, utilisez la combinaison de touches (Alt) (T) pour en tester le fonctionnement sans rendre votre choix définitif. Si la souris ne réagit pas comme vous le souhaitez, choisissez un autre type à l'aide du clavier et procédez à un nouveau test. Utilisez les touches (Tab) et (Entrée) pour rendre ce choix permanent.

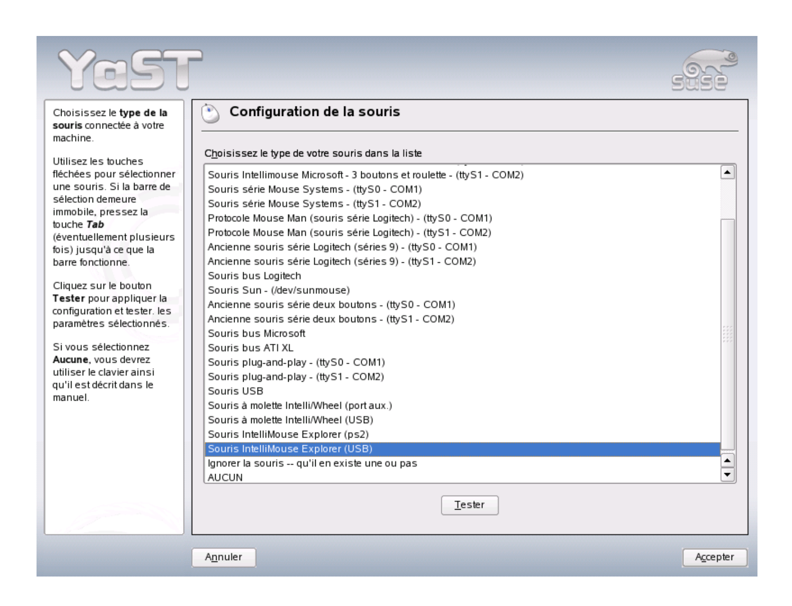


FIG. *1.5: Choix du type de souris*

1.5.4 Partitionnement

Dans la majorité des cas, la proposition de partitionnement faite par YaST est judicieuse et vous pouvez l'accepter sans la modifier. Cependant, si vous souhaitez un partitionnement spécial du disque dur, nous vous décrivons ci-après comment procéder.

Types de partition

Chaque disque dur contient une table des partitions qui a de la place pour quatre entrées. Chaque entrée dans la table des partitions peut être soit une partition primaire, soit une partition étendue. Cependant, il est impossible d'avoir plus d'une partition étendue.

Les partitions primaires sont très simples à considérer : elles sont constituées d'une suite continue de cylindres (zones physiques du disque) auquel un système d'exploitation est attribué. Cependant, vous ne pouvez créer que jusqu'à quatre partitions primaires par disque dur ; on ne peut pas en déclarer plus dans la table des partitions. Si vous avez besoin de plus de partitions, vous devrez créer une

partition étendue. Une partition étendue est également constituée d'une suite continue de cylindres du disque dur. Cependant, on peut encore diviser une partition étendue en plusieurs *partitions logiques* qui ne nécessitent aucune entrée dans la table des partitions. La partition étendue est, en quelque sorte, un conteneur qui comprend les partitions logiques.

Si vous avez besoin de plus de quatre partitions, vous devez vous assurer, lors du partitionnement qu'une des partitions, la quatrième en dernier lieu, est bien prédéfinie comme partition étendue afin de pouvoir lui attribuer l'ensemble des domaines de cylindres libres. Vous pourrez ensuite y définir autant de partitions logiques que vous le désirez (dans la limite de 15 partitions pour les disques SCSI, SATA et Firewire et de 63 partitions pour les disques (E)IDE. Le type de partition (primaire ou logique) sur laquelle l'installation de SUSE LINUX est effectuée n'est pas important.

Astuce

Disques durs avec identifiant de disque GPT

Pour les architectures qui utilisent l'identifiant GPT, le nombre de partitions primaires n'est pas limité. Il n'y a donc pas de partitions logiques dans ce cas.

Astuce

Espace disque nécessaire

Si vous laissez YaST procéder au partitionnement du disque dur, vous n'aurez (pratiquement) pas à vous préoccuper des besoins en espace disque et du partitionnement du disque dur. Au cas où vous procèderiez vous-même au partitionnement de votre disque dur, nous vous donnons ici quelques conseils quant à l'espace nécessaire aux différents types de système.

Système minimal : 500 Mo Ce système n'a pas d'interface graphique (X11), c'est à dire que vous ne pouvez travailler que depuis la console. En outre, vous ne pouvez procéder qu'à l'installation des logiciels les plus élémentaires.

Système minimal avec interface graphique : 700 Mo
Ici, vous pouvez installer X11 et quelques applications.

Système par défaut : 2,5 Go Vous pouvez ici installer des interfaces graphiques modernes telles que KDEou GNOME ainsi que des applications plus gourmandes comme, par exemple, OpenOffice, Netscape ou Mozilla.

La façon de créer les partitions dépend de l'espace disque disponible. Voici quelques indications simples :

Jusqu'à environ 4 Go : Une partition d'échange (swap) et une partition racine (`/`). La partition racine contient alors également les répertoires pour lesquels des partitions propres sont créées dans le cas de disques durs plus grands.

Plus de 4 Go : Une partition d'échange, une partition racine (1 Go) et une partition pour chacun des répertoires `/usr` (4 Go ou plus), `/opt` (4 Go ou plus) et `/var` (1 Go). Si vous ne désirez pas de partition séparée pour ces répertoires, ajoutez l'espace disque suggéré à la partition racine. Le reste de l'espace disponible peut être utilisé pour `/home`.

Selon votre matériel, il peut être nécessaire de configurer une partition d'amorçage (`/boot`) qui contiendra les fichiers d'amorçage et le noyau Linux. Cette partition doit se situer au début du disque et faire au moins 8 Mo ou un cylindre. En principe, si YaST a suggéré au départ de créer une telle partition, nous vous conseillons de le faire. Si vous hésitez, il vaut mieux créer une partion d'amorçage par prudence.

Vous devez songer que certaines applications, pour la plupart des programmes commerciaux, installent leurs données dans `/opt`. Par conséquent, pensez soit à prévoir une partition séparée pour `/opt`, soit à redimensionner la partition racine pour qu'elle ait une taille suffisante. KDE et GNOME sont également installés dans le répertoire `/opt`.

Partitionnement avec YaST

Quand vous choisissez le partitionnement dans la page de suggestions pour la première fois, la page de partitionnement de YaST apparaît avec les réglages actuels. Vous avez la possibilité d'accepter, de modifier ou de rejeter complètement la suggestion qui vous est faite pour procéder à une nouvelle distribution de l'espace disque.

Si vous choisissez 'Accepter la proposition de partitionnement', rien ne sera changé dans le schéma de partitionnement. Si vous choisissez 'Changer la proposition de partitionnement', la page de 'Partitionnement en mode expert' apparaît. Elle est expliquée dans la section 2.7.5 page 75). Le partitionnement proposé au début par YaST est affiché dans cette page comme point de départ pour vos modifications.

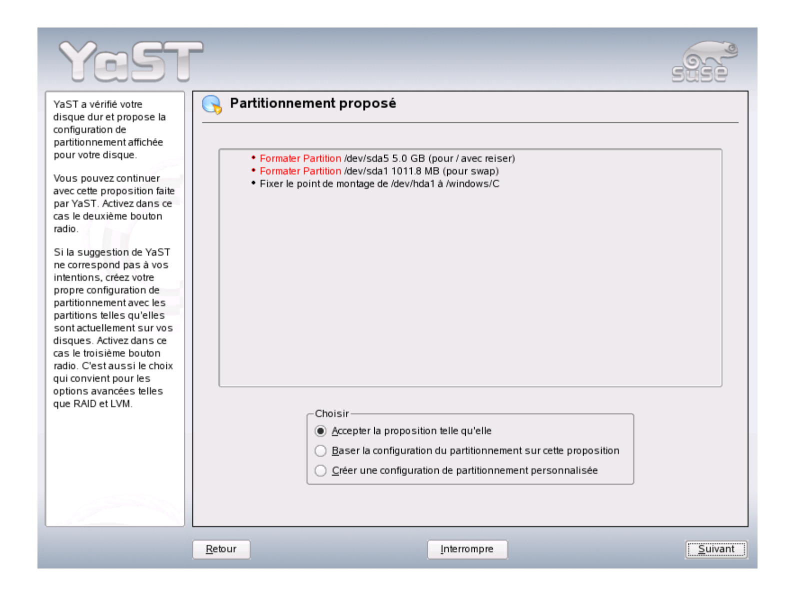


FIG. 1.6: *Modifier la proposition de partitionnement*

Si vous choisissez 'Créer partitions personnalisées', une page apparaît comme dans la figure 1.7 page suivante. Utilisez la liste pour choisir parmi les disques durs présents dans votre systèmes celui sur lequel SUSE LINUX sera installé.

Après avoir choisi un disque dur, vous pouvez préciser si vous désirez 'Utiliser la totalité du disque dur' ou si l'installation doit se faire sur des partitions existantes (s'il y en a). Si le disque dur choisi contient déjà un système d'exploitation Windows, il vous sera demandé si vous voulez effacer votre système Windows ou réduire sa taille. Avant de le faire, lisez la section Redimensionner une partition Windows page suivante. Si vous le souhaitez, vous passerez à la page de 'Partitionnement en mode expert' dans laquelle vous pourrez définir un schéma de partitionnement personnalisé (voir la section 2.7.5 page 75).

Avertissement

Utiliser tout le disque dur pour l'installation

Si vous choisissez 'Utiliser la totalité du disque dur', vous perdrez toutes les données présentes sur ce disque dur avant l'installation.

Avertissement

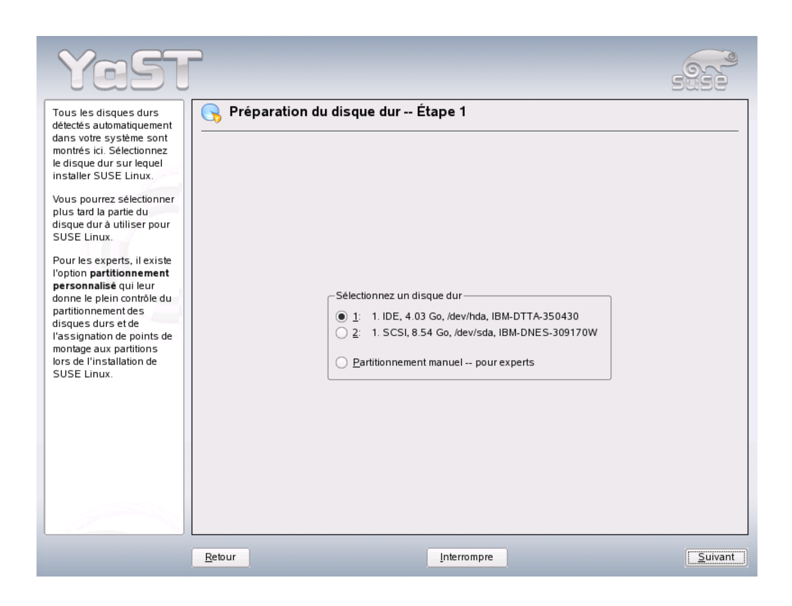


FIG. *1.7: Choix du disque dur*

Au cours des prochaines étapes de l'installation, YaST vérifiera si l'espace disque est suffisant pour la sélection de logiciels actuelle. Si ce n'est pas le cas, la sélection de logiciels sera automatiquement modifiée et la page de propositions vous en informera. Si vous disposez de suffisamment d'espace disque, YaST acceptera vos paramètres de configuration et partitionnera le disque dur en conséquence.

Redimensionner une partition Windows

Si, lors du partitionnement, vous avez choisi un disque dur contenant une partition Windows FAT ou NTFS comme destination de l'installation, YaST vous permet de supprimer ou de réduire cette partition. De cette façon, vous pourrez installer SUSE LINUX même s'il n'y a pas suffisamment d'espace libre sur le disque dur. C'est particulièrement utile lorsqu'il n'existe, sur le disque dur choisi, qu'une seule partition Windows occupant tout le disque, ce qui est parfois le cas sur les ordinateurs où Windows est livré préinstallé. Si YaST remarque que l'espace disponible sur le disque dur choisi est trop petit pour l'installation mais que ce problème peut être résolu en supprimant ou en réduisant une partition Windows, une page apparaît dans laquelle vous pouvez choisir une de ces deux options.

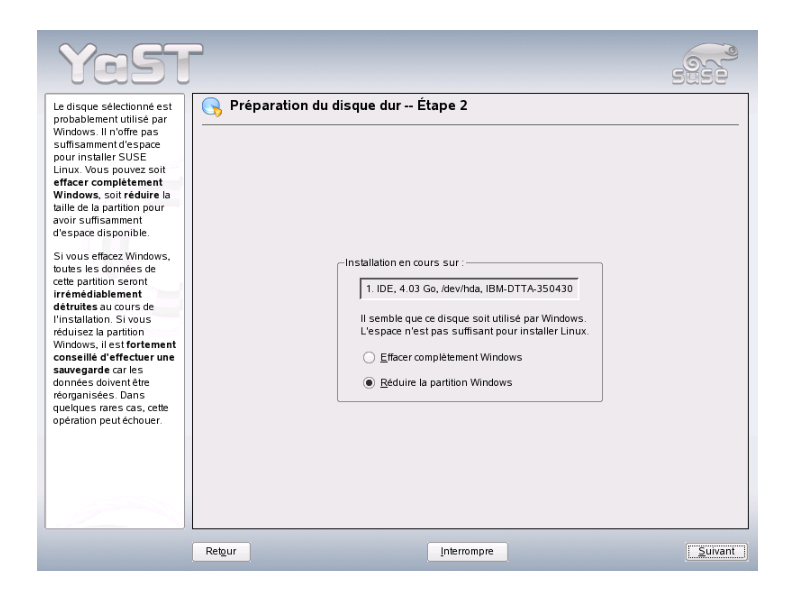


FIG. 1.8: *Options possibles pour les partitions Windows*

Si vous choisissez 'Supprimer Windows complètement', la partition Windows sera éliminée et l'espace libre ainsi gagné sera utilisée pour installer SUSE LINUX.

Avertissement

Effacer Windows

Si vous décidez d'éliminer Windows, notez que vous perdrez irrémédiablement toutes les données Windows lors du formatage.

Avertissement

Si vous décidez de réduire la partition Windows, interrompez d'abord l'installation puis amorcez Windows pour y procéder à certaines étapes préliminaires. Ceci n'est pas absolument nécessaire pour les partitions FAT, mais cela accélère le processus de réduction de la partition FAT et le rend plus sûr. Par contre, ces étapes sont vitales dans le cas des partitions NTFS.

Système de fichiers FAT Sous Windows, lancez tout d'abord le programme scandisk pour vous assurer que le système de fichiers FAT n'a pas de frag-

ments de fichiers perdus ou de liens croisés. Puis, lancez defrag pour déplacer les fichiers au début de la partition. Cela permet d'accélérer le redimensionnement de la partition sous Linux.

Si vous avez optimisé les paramètres de mémoire virtuelle sous Windows de manière à utiliser un fichier d'échange contigu ayant la même limite supérieure et inférieure, vous pouvez passer par une étape supplémentaire. Avec ces paramètres de Windows, le redimensionnement pourrait morceler et disperser le fichier d'échange sur toute la partition FAT. Il faudrait aussi complètement déplacer le fichier d'échange pendant le redimensionnement, ce qui ralentirait le processus. Il est donc préférable de désactiver ces optimisations de Windows pour le moment et de les réactiver une fois le redimensionnement terminé.

Système de fichiers NTFS Exécutez scandisk puis defrag sous Windows pour déplacer les fichiers au début de la partition. Contrairement au cas du système de fichiers FAT, vous devez absolument passer par ces étapes sans quoi la partition NTFS ne peut pas être redimensionnée.

Important

Réduire le fichier d'échange (swap) de Windows

Si vous utilisez votre système avec un fichier d'échange (swap) permanent sur un système de fichiers NTFS, il est possible que ce fichier soit situé à la fin du disque dur et y reste malgré l'exécution de defrag. Il peut alors être impossible de réduire suffisamment la partition. Pour résoudre ce problème, désactivez temporairement le fichier d'échange (la mémoire virtuelle sous Windows). Une fois la partition redimensionnée, réactivez la mémoire virtuelle.

Important

Une fois que vous aurez effectué ces préparatifs, choisissez l'option 'Redimensionner la partition Windows' dans la page de partitionnement. Après une rapide vérification, YaST ouvre une nouvelle page et vous fait une suggestion pour une réduction raisonnable de votre partition Windows.

Dans le premier diagramme à barres, YaST montre l'espace occupé actuellement par Windows ainsi que l'espace encore disponible sur le disque dur. Le second diagramme vous montre comment l'espace serait occupé après le redimensionnement tel que proposé par YaST. Reportez-vous à figure 1.9 page ci-contre. Vous pouvez accepter ce nouveau partitionnement ou utiliser la glissière pour modifier les dimensions des partitions (dans certaines limites).

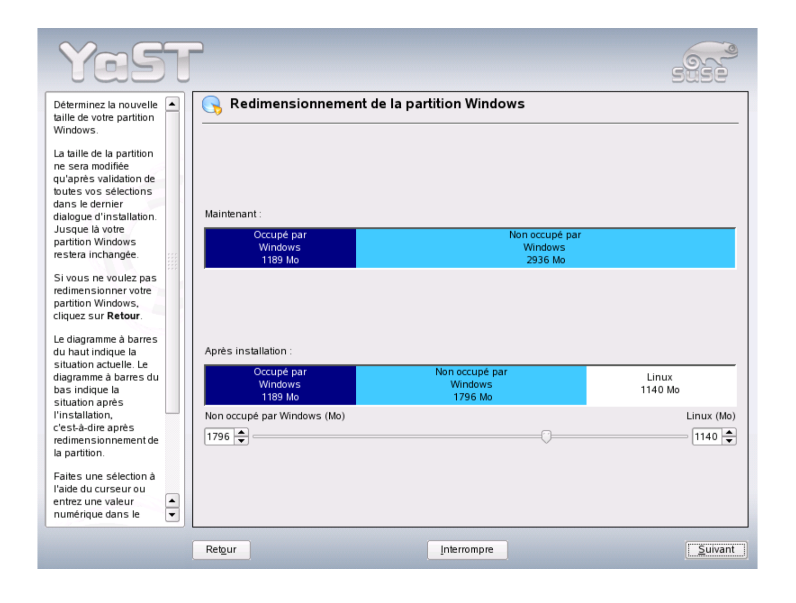


FIG. 1.9: *Redimensionner la partition Windows*

Si vous quittez cette page avec 'Suivant', la configuration actuelle sera enregistrée et vous retournerez à la page précédente. La réduction ne sera pas effectuée immédiatement, mais plus tard, juste avant le formatage du disque dur.

Important

Windows avec système de fichiers NTFS

Par défaut, les versions NT, 2000 et XP de Windows utilisent le système de fichiers NTFS. Les systèmes de fichiers NTFS, au contraire des systèmes de fichiers FAT, ne peuvent qu'être lus par Linux. Cela signifie que vous pouvez lire vos fichiers Windows depuis Linux, mais que vous ne pouvez pas les modifier. Si vous voulez accéder en écriture à vos données Windows et si vous n'avez pas besoin du système de fichiers NTFS, réinstallez Windows sur un système de fichiers FAT32. Vous aurez alors un accès complet à vos données Windows depuis SUSE LINUX.

Important

1.5.5 Logiciels

SUSE LINUX contient un grand nombre de paquetages logiciels pour divers domaines d'application. Étant donné qu'il serait très pénible de sélectionner un à un les paquetages SUSE LINUX offre trois types de systèmes avec différentes sélections de logiciels. En fonction de l'espace disque disponible, YaST choisit automatiquement un de ces types de système et l'affiche dans la zone de suggestion.

Système minimal (conseillé uniquement pour des utilisations spéciales)
: Ici, seul le système d'exploitation sera installé ainsi que différents services. Aucune interface graphique n'est installée, l'ordinateur n'est contrôlé que par l'intermédiaire de consoles ASCII. Ce type de système est particulièrement indiqué pour des serveurs qui ne nécessitent que peu ou pas d'interactions avec l'utilisateur.

Système graphique minimal (sans GNOME ou KDE)
: Si vous ne souhaitez pas utiliser le bureau KDE ou GNOME ou si vous n'avez pas assez d'espace, installez ce type de système. Le système installé dispose d'un environnement graphique élémentaire avec un gestionnaire de fenêtres. Vous pouvez utiliser tous les programmes qui ont leur propre interface graphique. Les programmes bureautiques ne sont pas installés.

Système par défaut avec GNOME et suite bureautique
: C'est un des systèmes prédéfinis les plus complets. Il contient le bureau GNOME ainsi que la majorité des programmes GNOME et des applications bureautiques.

Système par défaut avec KDE et suite bureautique
: Un tel système comprend le bureau KDE ainsi que la majorité des programmes de KDE et des applications bureautiques.

Si vous cliquez sur 'Logiciels' dans la fenêtre de suggestions, vous ouvrez une page dans laquelle vous pouvez choisir un des systèmes prédéfinis. Pour modifier l'étendue de l'installation, lancez le module de sélection de logiciels, c'est à dire le gestionnaire de paquetages, en cliquant sur 'Sélection détaillée' Reportez vous à la figure 1.10 page suivante.

Modifier la sélection de logiciels prédéfinie

Si vous installez le système par défaut, il n'est normalement pas nécessaire de modifier la sélection de paquetages, étant donné que le système définit un ensemble de logiciels cohérent qui devraient répondre aux besoins les plus courants sans modification. Cependant, il existe la possibilité de procéder à des modifications manuelles à l'aide du gestionnaire de paquetages. Ce gestionnaire vous

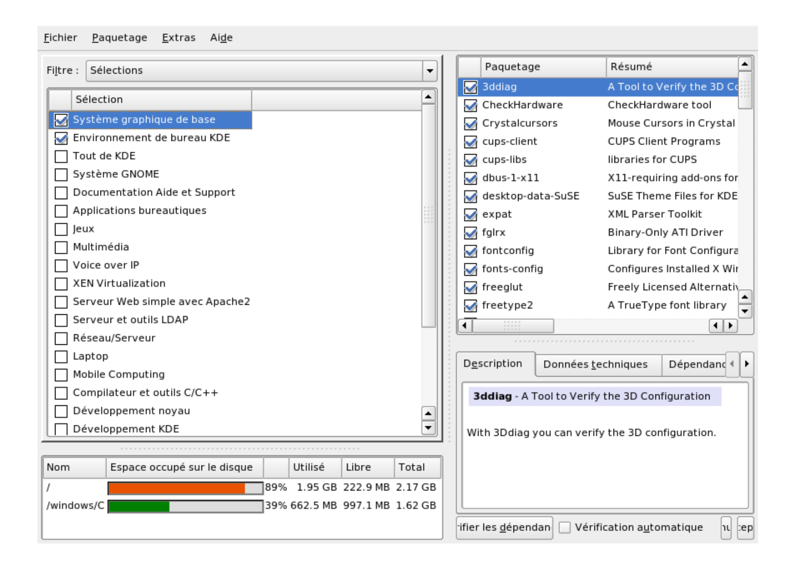


FIG. 1.10: *Installer et éliminer des logiciels avec le gestionnaire de paquetages YaST*

offre des filtres qui vous permettent de sélectionner certains logiciels parmi les nombreux paquetages que contient SUSE LINUX en utilisant des différents critères.

La zone de sélection des filtres se trouve en haut à gauche sous la barre de menus. Lors du démarrage, le filtre de sélections est activé. Les sélections groupent les programmes selon leur domaine d'application, comme par exemple Multimédia et Bureautique. Sous ce panneau, vous voyez les différents groupes du filtre de sélections, dont certains qui sont déjà présélectionnés étant donné qu'ils font partie de l'installation standard de ce type de système. D'un clic de souris sur la case à cocher correspondante, vous pouvez sélectionner des groupes de paquetages dans leur intégralité, soit pour l'installation, soit pour la désinstallation.

Dans la fenêtre de droite, vous voyez la liste des différents paquetages appartenant à chaque sélection. À tous les paquetages correspond un état symbolisé dans la colonne au début de la ligne. Lors de l'installation, ce sont surtout les états 'Installer' et 'Ne pas installer' qui vous intéressent, c'est-à-dire respectivement une croix à droite du nom du paquetage ou un espace libre. Vous pouvez ici, sélectionner ou désélectionner chaque paquetage séparément. À cette fin, cliquez aussi souvent qu'il le faut sur le symbole d'état en début de ligne jusqu'à avoir atteint

l'état désiré.Vous pouvez également, en cliquant avec le bouton droit de la souris sur la ligne correspondant au paquetage, ouvrir un menu déroulant qui affiche tous les états. Les autres états seront expliqués en détails dans la description de ce module dans la section 2.2.1 page 39.

Autres filtres

Si vous déroulez la zone de sélection de filtres, vous verrez une sélection de filtres supplémentaires qui vous aideront à ordonner les paquetages. Pour l'installation, la sélection par 'Groupes de paquetages' est particulièrement intéressante. Avec ce filtre, les paquetages sont affichés sur le côté gauche et sont ordonnés par thème dans une structure en arborescence. Plus vous vous déplacez vers les extrémités des ramifications de l'arborescence dans les sous-groupes (thèmes), plus la sélection se précise, et par conséquent, plus le nombre de paquetages affichés à droite qui correspondent à cette sélection diminue.

La fonction de 'Recherche' vous sert à retrouver un paquetage déterminé. Vous trouverez des explications dans la section 2.2.1 page 39.

Dépendances de paquetages et conflits

Vous ne pouvez pas simplement installer n'importe quelle combinaison de paquetages logiciels. Les différents paquetages installés doivent être compatibles entre eux. Si cette règle n'est pas respectée, ils peuvent interférer l'un avec l'autre et provoquer des conflits qui mettent en danger le bon fonctionnement du système pris comme un tout. C'est pour cela que des avertissements relatifs aux dépendances non résolues et conflits entre paquetages peuvent apparaître dans cette page. Si vous installez SUSE LINUX pour la première fois ou si vous ne comprenez pas la signification de ces avertissements, veuillez lire la section 2.2.1 page 39. Vous y trouverez des informations détaillées quant à l'utilisation du gestionnaire de paquetage ainsi qu'une brève vue d'ensemble de l'organisation des logiciels sous Linux.

Avertissement

La sélection standard qui vous est proposée, fruit d'une longue expérience, est d'une manière générale très judicieuse pour une utilisation privée, que ce soit pour le débutant comme pour l'utilisateur plus averti. Normalement, il n'est pas nécessaire de procéder à des modifications. N'installez pas et surtout ne désinstallez pas de paquetages sans savoir exactement quelles en seront les conséquences. En tout état de cause, et surtout lorsque vous supprimez des paquetages, veillez à tenir compte des avertissements et ne supprimez surtout pas de paquetages du système de base Linux.

Avertissement

Quitter la sélection de logiciels

Lorsque vous êtes satisfait de votre sélection de logiciels et une fois qu'il n'existe plus de dépendances non résolues ou de conflits entre paquetages, cliquez sur 'Accepter' pour quitter le programme. Lors de l'installation, la sélecion de logiciels à installer sera enregistrée en attendant que la procédure d'installation proprement dite soit démarrée.

1.5.6 Configuration de l'amorçage

Lors de l'installation, YaST propose un mode d'amorçage approprié à votre système. Normalement, vous n'avez pas besoin de modifier ces paramètres. Cependant, modifiez la proposition du système en cas de besoins spéciaux de votre environnement système.

Vous pouvez, par exemple, configurer le mécanisme d'amorçage de façon à ce qu'il soit nécessaire d'insérer une disquette d'amorçage spéciale lors du démarrage de SUSE LINUX. Cela a l'inconvénient de nécessiter une disquette dans le lecteur à l'amorçage, mais permet de laisser le mécanisme d'amorçage existant intact. En général, ceci n'est pas nécessaire étant donné que YaST configure le chargeur d'amorçage de telle façon que vous puissiez amorcer le système d'exploitation de votre choix. Plus tard, vous pourrez également changer l'emplacement où le chargeur d'amorçage de SUSE LINUX est enregistré sur le disque dur.

Si vous voulez modifier la configuration d'amorçage proposée par YaST choisissez 'Amorçage du système'. Une page apparaît dans laquelle vous pouvez changer beaucoup de détails du mécanisme d'amorçage. Vous trouverez des informa-

tions à ce sujet dans la section 8.4 page 197. La modification du mode d'amorçage est à réserver à des utilisateurs expérimentés.

1.5.7 Fuseau horaire

Dans ce formulaire (voir la figure 1.11 de la présente page), vous pouvez, dans le champ 'Horloge interne réglée à', choisir entre les options `Heure locale` et `UTC` (Coordinated Universal Time). Votre choix dépend de la manière dont l'horloge matérielle (du BIOS) de votre ordinateur est configurée. Si elle est réglée sur le méridien de Greenwich, qui correspond à `UTC`, votre système SUSE LINUX se chargera de passer automatiquement entre l'heure d'été et l'heure d'hiver.

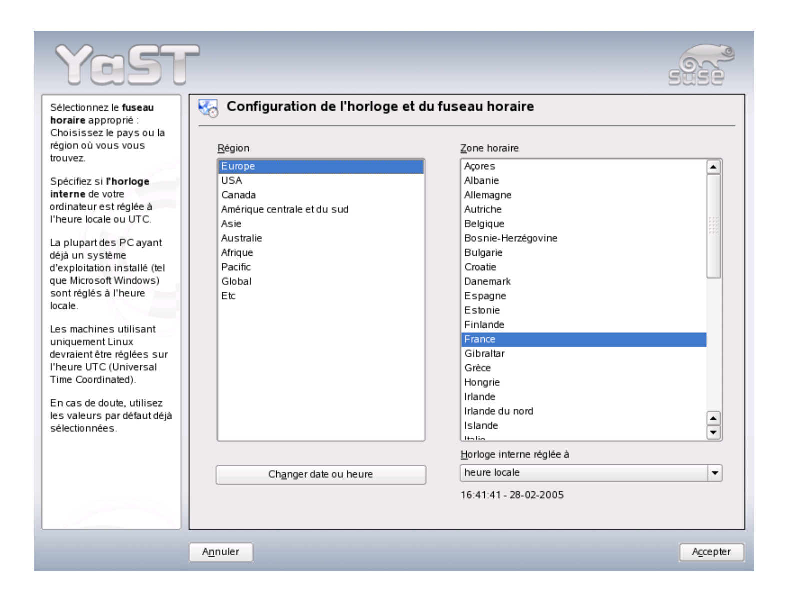


FIG. *1.11: Choix du fuseau horaire*

1.5.8 Langue

La langue a déjà été choisie au début de l'installation (voir la section 1.3 page 8. Cependant, vous pouvez modifier ce réglage ici et sélectionnez également toute

langue supplémentaire à installer sur votre système. Dans la partie supérieure de ce dialogue, sélectionnez la langue principale. Il s'agit de la langue qui sera activée après l'installation. Adaptez la configuration de votre clavier et de la zone horaire à la langue principale sélectionnée en activant les cases à cocher. Vous pouvez éventuellement configurer la langue pour l'utilisateur `root` en cliquant sur 'Détails'. Il existe trois options :

uniquement ctype La variable `LC_CTYPE` pour l'utilisateur `root` est enregistrée dans le fichier `/etc/sysconfig/language`. Ceci définit la localisation pour les appels de fonctions propres à chaque langue.

oui L'utilisateur `root` a exactement la même configuration de la langue que l'utilisateur local.

non La configuration de la langue de l'utilisateur `root` est indépendante du choix général de la langue. Toutes les définitions des variables `locales` seront annulées.

Certains administrateurs système ne souhaitent pas que le compte `root` fonctionnent en prenant en charge le support multilingue UTF-8. Si c'est le cas, désélectionnez 'Utiliser l'encodage UTF-8'.

La liste dans la partie inférieure du dialogue permet la sélection de langues additionnelles à installer. Pour toutes les langues sélectionnées dans cette liste, YaST vérifie s'il existe des paquetages spécifiques à ces langues pour les paquetages de votre sélection de logiciels actuelle. Si c'est le cas, ces paquetages seront installés.

Cliquez sur 'Accpeter' pour terminer la configuration ou sur 'Annuler' pour annuler vos modifications.

1.5.9 Procéder à l'installation

En cliquant sur 'Suivant', vous acceptez la suggestion avec toutes les modifications que vous avez effectuées et vous arrivez à un formulaire de confirmation. Si vous cliquez ici sur 'Oui', l'installation peut commencer avec les paramètres que vous avez choisis. Le processus d'installation dure généralement de 15 à 30 minutes, selon la performance de votre machine et la sélection de logiciels à installer. Après l'installation des paquetages, YaST amorce le système installé et vous pouvez ensuite passer à la configuration du matériel et des services.

1.6 Terminer l'installation

Une fois que le système de base a configuré et que tous les logiciels sélectionnés ont été installés, indiquez un mot de passe pour l'administrateur du système (utilisateur `root`). Vous pourrez alors configurer l'accès à Internet et la connexion au réseau. Si votre connexion à l'Internet fonctionne, vous pourrez procéder à la mise à jour du système dès l'installation. Vous pouvez également configurer un sereur d'authentification pour gérer de façon centralisée les utilisateurs en réseau local. Finalement, configurez le matériel connecté.

1.6.1 Mot de passe root

Le super-utilisateur (appelé également administrateur du système) se nomme root . `root` a des droits sur le système que les autres utilisateurs n'ont pas forcément. Il peut tout faire sans restriction : modifier la configuration du système, installer de nouveaux programmes ou mettre en place de nouveaux composants matériels. Si un utilisateur a oublié son mot de passe s'il a des problèmes avec le système, `root` peut l'aider. En règle générale, on ne devrait se connecter sous le compte `root` que pour exécuter des tâches d'administration, des travaux de maintenance ou de réparation. Se connecter ainsi pour le travail quotidien est plutôt risqué, car `root` peut, en une seule erreur, faire perdre irrémédiablement de nombreux fichiers système.

Le mot de passe de `root` doit être saisi une seconde fois afin d'être vérifié (voir la figure 1.12 page ci-contre). Mémorisez bien le mot de passe de l'utilisateur `root`. Une fois que vous l'aurez saisi, il ne vous sera plus possible de le retrouver.

Avertissement

L'utilisateur root

L'utilisateur `root` a tous les droits et peut apporter toutes sortes de modifications au système. Si vous voulez vous charger de tâches impliquant des modifications, il vous faut un mot de passe attribué spécialement à `root`. Sans ce mot de passe, il ne vous sera pas possible d'exécuter des tâches d'administration.

Avertissement



FIG. 1.12: *Régler le mot de passe de root*

1.6.2 Configuration réseau

Vous pouvez maintenant configurer n'importe quel périphérique réseau (cartes réseau, modems et matériel RNIS ou DSL) pour relier votre système au reste du monde. Si votre système dispose de ce type de matériel, profitez de cette opportunité maintenant. En effet, une connexion à Internet permettre à YaST de télécharger des mises à jour pour SUSE LINUX qui seront prises en compte lors de l'installation.

Si vous souhaitez configurer ici votre matériel réseau, reportez-vous à la section 22.4 page 433. Sinon, choisissez l'option 'Ignorer la configuration réseau' et cliquez sur 'Suivant'. Vous pourrez configurer vos composants réseau ultérieurement après avoir terminé l'installation du système.

1.6.3 Configuration du pare-feu

Dès que vous mettez en réseau votre système, un pare-feu est démarré automatiquement sur l'interface configurée. Les paramètres de configuration du pare-feu



FIG. 1.13: *Configurer les périphériques réseau*

sont affichés dans la page de configuration du réseau. À chaque modification de la configuration des interfaces ou des services, la proposition de configuration pour le pare-feu est actualisée automatiquement. Si vous souhaitez adapter les paramètres générés automatiquement à vos propres besoins, cliquez sur 'Modifier' → 'Pare-feu'.

Dans la page qui apparaît, déterminez si le pare-feu doit être démarré ou non. Si vous ne souhaitez pas démarrer le pare-feu, indiquez-le dans l'option correspondante et quittez la page. Pour démarrer le pare-feu et en modifier la configuration, cliquez sur 'Suivant' et une suite de pages semblables à celles qui sont décrites dans la section Configuration avec YaST page 635 commence.

1.6.4 Tester la connexion Internet

Si vous avez configuré une connexion Internet, vous pouvez maintenant vérifier que celle-ci fonctionne correctement. À cette fin, YaST établit une connexion avec le serveur de SUSE et vérifie par la même occasion si des mises à jour sont disponibles pour SUSE LINUX. Si la connexion fonctionne correctement, vous pouvez

télécharger ces mises à jour dans l'étape suivante. En outre, les notes relatives à la dernière version disponible sur le serveur SUSE seront également téléchargées et elles seront affichées à l'écran à la fin de l'installation.



FIG. 1.14: *Tester la connexion Internet*

Si vous ne souhaitez pas procéder ici au test de la connexion Internet, choisissez 'Ignorer ce test' et cliquez sur 'Suivant'. Le téléchargement des mises à jour et des notes les plus récentes ne se fera pas non plus.

1.6.5 Télécharger des mises à jour des logiciels

Si YaST a pu établir une connexion Internet avec les serveurs de SUSE dans l'étape précédente, vous aurez la possibilité de procéder à une mise à jour en ligne avec YaST. De cette façon, les éventuels correctifs de correction d'erreurs et de problèmes de sécurité connus seront installés.

Important

Téléchargement des mises à jour des logiciels

Le téléchargement des mises à jour peut prendre un certain temps qui dépendra du débit de la connexion à Internet ainsi que de la taille des fichiers de la mises à jour.

Important

Si vous souhaitez mettre immédiatement à jour les logiciels, choisissez 'Procéder maintenant à la mise à jour' et cliquez sur 'OK'. Vous entrez dans la page de mise à jour en ligne de YaST où vous pouvez voir une liste des correctifs disponibles, les sélectionner et les appliquer. Pour plus d'informations sur cette procédure, reportez-vous à la section 2.2.3 page 50. Vous pouvez aussi procéder à la mise à jour plus tard, après l'installation. Dans ce cas, cochez 'Ignorer la mise à jour' et cliquez sur 'OK'.

1.6.6 Authentification des utilisateurs

Si vous avez configuré une connexion Internet dans le cadre de l'installation, vous avez maintenant quatre possibilités pour administrer les utilisateurs du système installé.

Administration locale des utilisateurs
Les utilisateurs sont administrés localement sur l'ordinateur installé. C'est la méthode conseillée pour les ordinateurs isolés. Dans ce cas, les données des utilisateurs sont administrées au moyen du fichier local `/etc/passwd`.

LDAP Les utilisateurs de tous les systèmes sont administrés en réseau, de façon centrale, sur un serveur LDAP.

NIS Les utilisateurs de tous les systèmes en réseau sont administrés de façon centralisée sur un serveur NIS.

Samba Une authentification SMB est souvent utilisée dans les réseaux hétérogènes Linux et Windows.

Si toutes les conditions sont remplies, YaST ouvre une page permettant de choisir la méthode d'administration des utilisateurs, comme dans la figure 1.15 page ci-contre. Si vous n'êtes pas connecté en réseau, créez des comptes d'utilisateurs locaux.

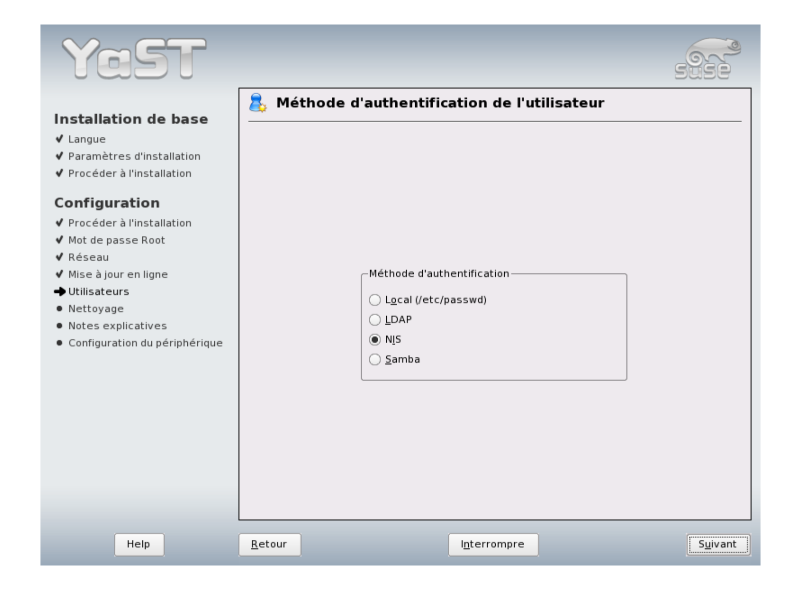


FIG. *1.15: Authentification des utilisateurs*

1.6.7 Configuration en tant que client NIS

Si vous avez décidé d'administrer les utilisateurs au moyen de NIS, l'étape suivante consiste à configurer un client NIS. Nous ne décrivons ici que la configuration d'un client ; vous trouverez des informations sur la configuration d'un serveur NIS avec YaST dans le chapitre 25 page 485.

Dans le dialogue suivant (voir la figure 1.16 page suivante), précisez tout d'abord si le client NIS dispose d'une adresse IP statique ou d'une adresse IP dynamique assignée par DHCP. Si vous choisissez DHCP, vous ne pouvez pas indiquer de domaine NIS ni l'adresse IP du serveur NIS puisque ces données seront également fournies par DHCP. Vous trouverez plus d'informations sur le protocole DHCP dans le chapitre 27 page 499. Si le client dispose d'une adresse IP statique, indiquez le domaine et le serveur NIS manuellement.

Activez l'option de diffusion générale dans la case à cocher correspondante pour permettre la recherche d'un serveur NIS dans le réseau dans le cas où le serveur indiqué ne répondrait pas. Vous avez également la possibilité d'indiquer différents domaines avec un domaine par défaut. Avec l'option 'Modifier', vous pou-

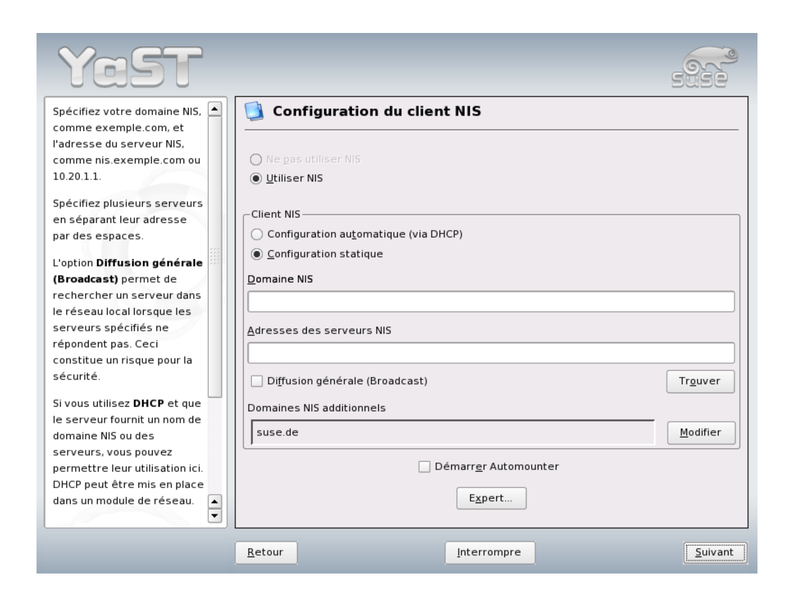


FIG. *1.16: Configuration d'un client NIS*

vez également indiquer plusieurs serveurs avec fonction de diffusion générale pour chaque domaine.

La configuration pour experts vous permet de sélectionner l'option 'Répondre uniquement à l'hôte local' afin d'éviter que d'autres ordinateurs du réseau puissent savoir quel serveur utilise son client. Si vous activez 'Serveur défectueux', les réponses d'un serveur seront également acceptées sur un port non privilégié. Vous pourrez trouver plus d'informations à ce sujet dans la page de manuel de `ypbind`.

1.6.8 Créer des utilisateurs locaux

Si vous avez décidé que les utilisateurs ne seront pas authentifiés au moyen d'un serveur d'authentification, vous avez ici l'opportunité de créer des utilisateurs locaux. Les données de ces utilisateurs (nom, nom d'utilisateur, mot de passe, etc.) sont enregistrées et administrées sur le système installé.

Linux est un système d'exploitation qui permet à plusieurs utilisateurs de travailler simultanément sur un seul et même système. Chaque utilisateur a besoin

d'un compte d'utilisateur sous lequel il se connectera au système. Le système des comptes d'utilisateurs est une excellente mesure de sécurité pour le système. Ainsi, il n'est pas possible à des utilisateurs ordinaires de modifier ou d'effacer d'importants fichiers système. Par ailleurs, les données personnelles des utilisateurs ne peuvent pas être modifiées, regardées, voire falsifiées par d'autres utilisateurs. Les utilisateurs peuvent mettre en place leur propre environnement de travail qu'ils retrouveront inchangé chaque fois qu'ils se connecteront à nouveau au système Linux.



FIG. 1.17: *Définir le nom d'utilisateur et le mot de passe*

Vous pouvez créer un tel compte d'utilisateur dans la page qui vous est présentée dans la figure 1.17 de la présente page. Après avoir saisi votre prénom et votre nom, choisissez un nom d'utilisateur pour le système (login). Vous pouvez cliquer sur 'Suggestion' pour générer automatiquement un nom d'utilisateur.

Il vous faut enfin indiquer un mot de passe pour l'utilisateur. Vous devrez le saisir une seconde fois pour être sur que vous n'avez pas saisi quelque chose d'autre par erreur. Le nom d'utilisateur sert à dire au système qui vous êtes et le mot de passe lui permet de s'assurer qu'il s'agit bien de vous.

Avertissement

Nom d'utilisateur et mot de passe

Notez soigneusement votre nom d'utilisateur et votre mot de passe. Vous en aurez besoin lors de chaque connexion au système.

Avertissement

Pour constituer une protection efficace, un mot de passe devrait avoir une longueur comprise entre cinq et huit caractères. La longueur maximale d'un mot de passe est de 128 caractères. Cependant, un module spécial est alors nécessaire. Si ce module n'a pas été chargé, seuls les huit premiers caractères sont utilisés pour l'identification. Il est tenu compte de la casse des lettres et il convient donc de différencier majuscules et minuscules. Les caractères accentués ne sont pas admis mais les caractères spéciaux ainsi que les chiffres de 0 à 9 peuvent être utilisés.

Pour les utilisateurs locaux, il existe encore deux options qui peuvent être activées au choix.

'Recevoir des messages du système' Si vous activez cette case à cocher, vous recevrez les messages de services du système. Normalement, ces messages ne sont envoyés qu'à l'administrateur `root`. Cependant, étant donné que vous n'êtes connecté qu'exceptionnellement en tant que `root`, cette option est surtout intéressante pour l'utilisateur qui travaille le plus souvent sur ce système

'Connexion automatique' Cette option n'est disponible que si vous utilisez le bureau KDE. Avec elle, l'utilisateur actuel est connecté automatiquement lors du démarrage du système. Ceci est surtout intéressant lorsque l'ordinateur n'est utilisé que par une personne.

Avertissement

Connexion automatique

Lors de la connexion automatique, lorsque le système démarre, il lance un environnement de bureau directement sous votre compte d'utilisateur, sans aucune procédure d'authentification. N'utilisez pas cette option si d'autres gens ont également accès à cet ordinateur et si il contient des données confidentielles.

Avertissement

1.6.9 Notes de version

Après avoir configuré l'authentification des utilisateurs, vous verrez apparaître les notes de version. Prenez le temps de les lire car elles contiennent des informations actuelles qui n'étaient pas encore disponibles lors de l'impression de ce manuel. Si vous avez configuré une connexion Internet et avez vérifié son fonctionnement avec le serveur de SUSE, vous avez obtenu la dernière version de SUSE ainsi que les informations de dernière minute.

1.7 Configuration du matériel

Après l'installation, YaST vous présente encore une page dans laquelle vous pouvez configurer votre carte graphique ainsi que différents composants matériels du système , tels que l'imprimante ou la carte son. En cliquant sur le nom des différents composants, vous démarrez la configuration du matériel. YaST détecte et configure alors automatiquement les composants matériels.

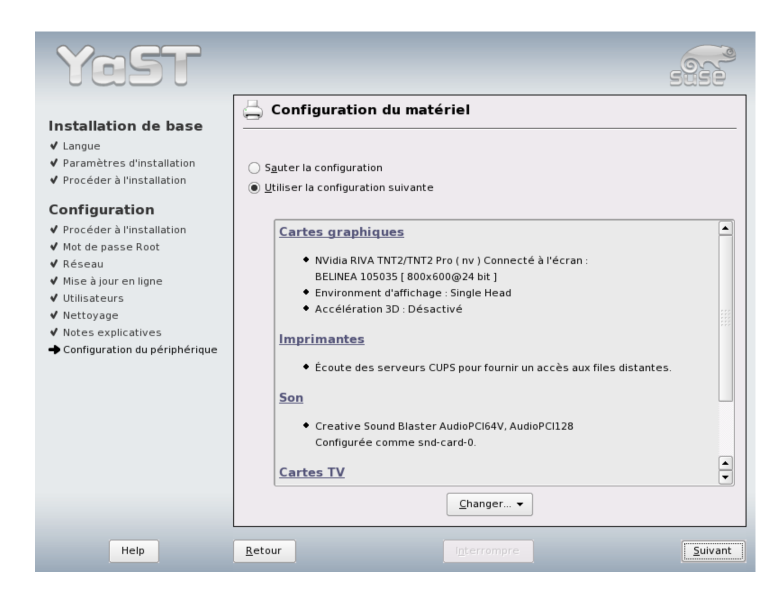


FIG. *1.18: Configurer les composants du système*

Vous pourrez procéder à la configuration des périphériques plus tard, mais nous vous recommandons de configurer la carte graphique tout de suite. Les réglages de l'affichage configurés automatiquement par YaST conviennent la plupart du temps, mais les préférences concernant la résolution, le nombre de couleurs et les autres caractéristiques d'affichage varient beaucoup d'un utilisateur à un autre. Si vous souhaitez changer ces réglages, choisissez l'option 'Cartes graphiques'. La procédure de configuration est décrite dans la section 11.1 page 234. Une fois que YaST a écrit les fichiers de configuration, cliquez dans la dernière page sur 'Terminer' pour terminer l'installation de SUSE LINUX.

1.8 Connexion en mode graphique

SUSE LINUX est maintenant installé. Si, dans le cadre de l'administration locale des utilisateurs, vous avez activé la connexion automatique, vous pouvez commencer sans vous connecter. Sinon, vous verrez apparaître sur votre écran l'écran de connexion graphique comme dans la figure 1.19 de la présente page. Donnez votre nom d'utilisateur ainsi que votre mot de passe afin de vous connecter à votre système.

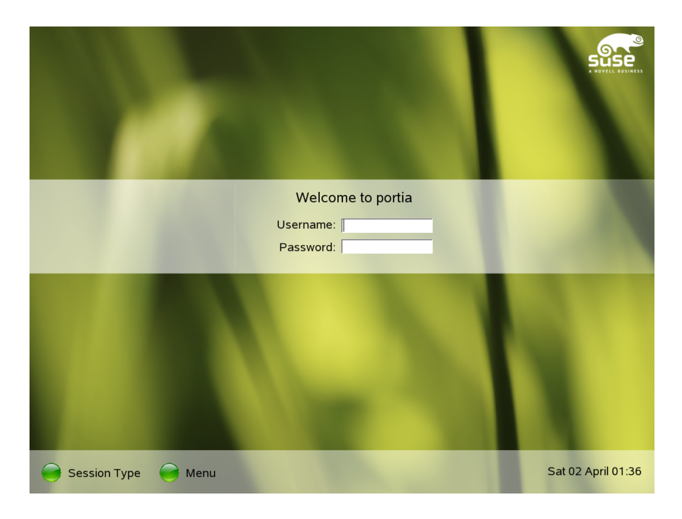


FIG. 1.19: *L'écran de connexion de KDM*

Configuration du système avec YaST

YaST (Yet another Setup Tool), dont vous avez déjà fait connaissance lors de l'installation, est également *l'outil* de configuration de SUSE LINUX. Ce chapitre décrit la configuration de votre système à l'aide de YaST. Vous pourrez configurer confortablement les composants du système les plus importants, c'est à dire, la plus grande partie du matériel, l'interface graphique, l'accès à Internet, les paramètres de sécurité, l'administration des utilisateurs, l'installation de logiciels ainsi que les mises à jour du système et les informations relatives à celui-ci. En outre, vous trouverez des instructions nécessaires à l'utilisation de YaST en mode texte.

La configuration du système avec YaST s'effectue à travers différents modules de YaST. Selon la plateforme matérielle utilisée et la sélection de logiciels installés, vous avez le choix entre différentes façons d'accéder à YaST dans le système installé.

Si vous utilisez une des deux interfaces graphiques KDE ou GNOME, démarrez le centre de contrôle de YaST avec le menu de SUSE ('Système' → 'YaST'). KDE intègre également les différents modules de configuration de YaST dans le centre de contrôle de KDE. Vous êtes appelé à saisir le mot de passe root avant que YaST ne démarre car celui-ci nécessite les droits de l'administrateur du système pour pouvoir modifier les fichiers système.

Depuis la ligne de commande, démarrez YaST avec les commandes `su` (pour vous connecter en tant qu'utilisateur `root`) puis `yast2`. Si vous souhaitez démarrer YaST en mode textuel, saisissez `yast` au lieu de `yast2`. En tant que `root`, utilisez également `yast` afin de démarrer le programme depuis une console virtuelle.

Astuce

Si vous désirez changer la langue de YaST, cliquez sur 'Système' dans le centre de contrôle de YaST puis sélectionnez la langue souhaitée dans le menu 'Sélectionner une langue'. Sélectionnez la langue, fermez le centre de contrôle de YaST, déconnectez-vous de votre système puis reconnectez-vous. Lorsque vous redémarrerez YaST, la nouvelle langue sera activée.

Astuce

Dans le cas des plateformes matérielles qui n'ont pas d'écran ou pour la maintenance à distance de systèmes depuis d'autres ordinateurs, exécutez YaST à distance. Ouvrez tout d'abord une console sur l'hôte sur lequel vous voulez exécuter YaST et saisissez, à l'invite, la commande `ssh -X root@<nom du système à configurer>`, afin de vous connecter en tant qu'utilisateur `root` sur le système à configurer et d'obtenir l'affichage de sorties du serveur X sur votre terminal. Dès que la connexion SSH a été établie, saisissez `yast2` à l'invite du système distant afin de démarrer le mode graphique de YaST.

Pour démarrer YaST en mode textuel sur un autre système, utilisez `ssh root@<nom du système à configurer>` pour ouvrir la connexion puis démarrez YaST avec la commande `yast`.

2.1 Le centre de contrôle de YaST

Lorsque vous démarrez YaST en mode graphique, vous voyez tout d'abord apparaître le centre de contrôle de YaST tel qu'il est représenté dans la figure 2.1 page suivante). Dans la partie gauche de l'écran, vous trouvez les sous-divisions 'Logiciels', 'Matériel', 'Système', 'Périphériques réseau', 'Services réseau', 'Sécurité et Utilisateurs', 'Système' et 'Divers'. En cliquant sur les icônes, vous obtiendrez, dans la partie de droite, l'affichage du contenu de la catégorie sélectionnée. Vous pourrez alors sélectionner le point de menu souhaité. Cliquez, par exemple, sur 'Matériel' puis, à droite sur 'Son', une fenêtre s'ouvre dans laquelle vous pouvez procéder à la configuration de la carte son. La configuration est généralement effectuée en plusieurs étapes. Dans les dialogues, passez à l'étape suivante au moyen d'un clic sur 'Suivant'.

La partie gauche du masque de dialogue de la plupart des modules affiche un texte d'aide qui vous explique les entrées que vous devez faire. Pour obtenir de l'aide dans les modules n'ayant pas un texte d'aide intégré, appuyez sur la touche F1 ou sélectionnez 'Aide' dans le menu. Après avoir fait les spécifications nécessaires, vous terminerez chaque étape de la configuration en cliquant, dans le dernier dialogue, sur le bouton 'Terminer'. La configuration sera alors enregistrée.

2.2 Logiciels

2.2.1 Installer et supprimer des logiciels

Ce module vous permet d'installer des applications supplémentaires, de les mettre à jour ou de les désinstaller. Sous Linux, les logiciels se présentent sous forme de paquetages. Normalement, un paquetage contient tout ce qui fait un programme complet : le programme lui-même, les fichiers de configuration et la documentation qui lui correspondent. Étant donné que, sous Linux, le code source d'un programme est généralement disponible, il existe normalement un paquetage correspondant avec les sources du programme. Ces sources ne sont pas nécessaires pour travailler avec le programme mais il peut être intéressant, dans certains cas, de les installer. Ainsi, vous pourrez générer une version de ce programme à votre mesure.

Certains paquetages dépendent de façon fonctionnelle d'autres paquetages. Dans ce cas, le programme d'un paquetage ne peut fonctionner correctement que

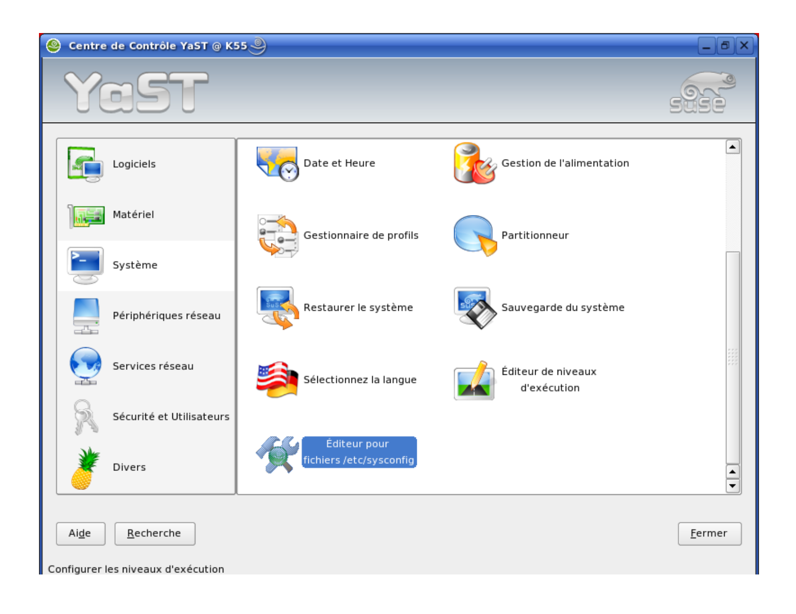


FIG. 2.1: *Le centre de contrôle de YaST*

lorsque l'autre paquetage est également installé. En outre, il existe aussi des paquetages qui exigent l'existence d'autres paquetages pour pouvoir être installés, parce que, par exemple, leur routine d'installation nécessite certains outils apportés par ce(s) autre(s) paquetage(s). Lorsque de tels paquetages doivent être installés, il faut prendre garde à observer un certain ordre lors de l'installation. En outre, il existe parfois plusieurs paquetages pouvant remplir la même fonction. Lorsque ces différents paquetages utilisent les mêmes ressources système, ils ne doivent pas être installés simultanément (conflit de paquetages). Ainsi, les dépendances et conflits peuvent non seulement exister entre deux paquetages mais peuvent aussi former de longues chaînes qui, dans les cas les plus complexes, sont très difficilement analysables. Les choses se compliquent encore si la bonne harmonie des programmes dépend aussi de leur version.

Toutes ces conditions doivent être vérifiées lors de l'installation, de la désinstallation ou de la mise à jour de logiciels. Heureusement, YaST dispose du module d'installation de logiciels ou gestionnaire de paquetages, un outil très performant pour la vérification des dépendances et conflits. Lorsqu'il est démarré, le gestionnaire de paquetages procède à une reconnaissance du système et affiche tous les

paquetages installés dans celui-ci. Lorsque vous sélectionnez des paquetages additionnels pour les installer, le gestionnaire de paquetages vérifie automatiquement (ou sur demande) les dépendances et les résout en ajoutant automatiquement les éventuels paquetages nécessaires. Si vous sélectionnez des paquetages qui entrent en conflit, le gestionnaire de paquetages vous en informe et vous propose une solution pour la résolution du conflit. Si vous sélectionnez pour le supprimer un paquetage nécessaire à d'autres paquetages, vous serez, de la même façon, informé par le gestionnaire de paquetages qui vous proposera aussi des informations détaillées ainsi que des propositions de solution.

Outre ces aspects purement techniques, le gestionnaire de paquetages est un bon outil pour obtenir un résumé de tous les paquetages disponibles dans SUSE LINUX. Ce résumé se réalise à l'aide de filtres qui procèdent à des regroupements thématiques et réduisent le nombre de paquetages affichés.

Le gestionnaire de paquetages

Pour modifier à l'aide du gestionnaire de paquetages les logiciels de votre système, sélectionnez 'Installer ou supprimer des logiciels' dans le centre de contrôle de YaST. Cette fenêtre de dialogue du gestionnaire de paquetages est représentée dans la figure 2.2 page suivante. La fenêtre est divisée en différentes zones thématiques. La taille de ces fenêtres a été optimisée, vous pouvez cependant les modifier en cliquant sur les lignes de séparation et en les déplaçant à l'aide de la souris. Nous allons vous décrire ici le contenu et l'utilisation de ces différentes zones.

La fenêtre de filtres

Le gestionnaire de paquetages vous propose différentes méthodes de filtrage qui regroupent les paquetages par catégories, affichant un nombre raisonnable de paquetages. La fenêtre de filtres est la zone à gauche sous la ligne de menu. Elle contrôle et affiche différentes méthodes de filtrage. Le contenu de la boîte de sélection de filtres située en haut détermine ce qui sera affiché dans la partie inférieure de la fenêtre de filtres. Cliquez sur la boîte de sélection de filtres pour afficher une liste des filtres disponibles et en sélectionner un.

Le filtre de sélections Lors du démarrage du gestionnaire de paquetages, le filtre de 'Sélections' est activé. Les sélections permettent de grouper les programmes selon leur utilité, par exemple multimédia ou bureautique. Sous la boîte de sélection des filtres, vous pouvez voir les différents groupes du filtre sélectionné dont ceux déjà installés sur votre système sont marqués.

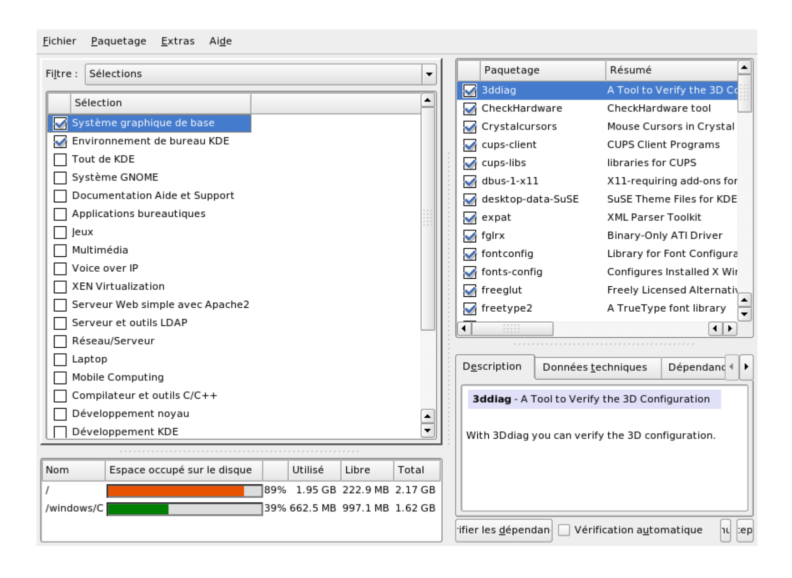


FIG. 2.2: *YaST~: le gestionnaire de paquetages*

En cliquant sur la boîte d'état au début de la ligne, vous pouvez sélectionner tous les état possibles successivement. L'état peut également être sélectionné directement en cliquant sur la ligne d'une sélection avec le bouton de droite de la souris pour faire apparaître le menu contextuel. La fenêtre de paquetages individuels à droite affiche tous les paquetages qui appartiennent à la sélection actuelle. Vous pouvez y sélectionner ou désélectionner individuellement les paquetages.

Le filtre de groupes de paquetages Une autre façon de filtrer est la sélection par 'Groupes de paquetages'. Ce filtre offre une gestion plutôt technique des paquetages et est destiné à des utilisateurs qui connaissent déjà un peu la structure des paquetages de SUSE LINUX. Les paquetages sont affichés à gauche dans une arborescence et regroupés selon des thèmes tels que applications, développement, matériel, etc. Plus vous avancez dans l'arborescence , plus le thème se précise et plus la liste correspondante de paquetages diminue, offrant ainsi une meilleure visibilité.

Une autre possibilité de ce filtre est l'affichage de *tous* les paquetages par ordre alphabétique. Pour cela, sélectionnez en haut l'option 'zzz tous'. Étant donné que SUSE LINUX contient énormément de paquetages, il est pos-

sible, selon les performances de votre matériel, que la création de cette liste prenne un certain temps.

La fonction de recherche La fonction de 'Recherche' est la méthode la plus simple pour retrouver un paquetage bien déterminé. À l'aide de critères de recherche adéquats, il est possible de définir votre recherche de façon si précise que vous pouvez réussir à ne faire afficher qu'un seul paquetage dans la liste des résultats. Pour cela, introduisez une chaîne de caractères et sélectionnez, à l'aide des cases à cocher, ou cette chaîne doit être recherchée (dans le nom uniquement, dans le nom et dans la description ou dans les dépendances entre paquetages). Pour leurs recherches, les experts peuvent même introduire des caractères jokers ou des expressions régulières et à l'aide des champs ″Fournit" et ″Nécessite" faire des recherches en fonction des dépendances de paquetages. Par exemple, cette fonction peut être utilisée pour vérifier quel paquetage contient une bibliothèque spécifique.

Astuce

Recherche rapide

Outre le filtre 'Recherche', il existe une fonction de recherche rapide dans chaque liste du gestionnaire de paquetages. Il suffit d'introduire l'initiale du nom d'un paquetage et le pointeur se positionne directement sur le premier paquetage de la liste dont le nom commence par ce caractère. Pour que cela fonctionne, la liste de paquetages doit être sélectionnée (d'un clic de souris).

Astuce

Langues Certains paquetages dans SUSE LINUX contiennent des paquetages spécifiques à la langue, par exemple, des textes traduits pour les programmes d'interface utilisateur, de la documentation et des fontes. Ce filtre affiche une liste de toutes les langues prises en charge par SUSE LINUX dans le fenêtre de gauche. Si vous sélectionnez une de ces langues, la fenêtre de droite affiche tous les paquetages disponibles dans cette langue. Parmi ceux-ci, tous les paquetages faisant partie de votre sélection de logiciels sont automatiquement marqués pour l'installation.

Note

Étant donné que certains paquetages spécifiques à la langue peuvent dépendre d'autres paquetages, le gestionnaire de paquetages pourra, dans ces cas, sélectionner des paquetages supplémentaires pour l'installation.

Note

Résumé de l'installation Après avoir sélectionné des paquetages pour les installer, les supprimer ou les mettre à jour, vous pouvez utiliser la boîte de sélection de filtres pour voir un résumé de l'installation et savoir ainsi précisément ce qui arrivera à chaque paquetage en cliquant sur 'Accepter'. Utilisez les cases à cocher à gauche pour filtrer les paquetages à voir dans la fenêtre d'affichage individuel des paquetages. Si, par exemple, vous souhaitez uniquement vérifier quels paquetages sont déjà installés, désactivez toutes les cases à cocher dès le démarrage à l'exception de 'Conserver'.

L'état des paquetages dans la fenêtre d'affichage individuel peut être modifié comme à votre habitude. Cependant un paquetage peut alors ne plus remplir les conditions du filtre de recherche. Si vous souhaitez également éliminer ces paquetages de la liste, actualisez celle-ci en cliquant sur 'Actualiser la liste'.

La fenêtre de paquetage

Selon le filtre sélectionné, la liste des paquetages affichés dans la fenêtre d'affichage individuel des paquetages diffère. Par exemple, si le filtre 'Sélections' est actif, les paquetages affichés sont ceux appartenant à la sélection faite.

Dans le gestionnaire de paquetages, chaque paquetage à un état logique qui définit ce qui doit arriver au paquetage, par exemple "Installer" ou "Supprimer". Comme dans le filtre de sélections, cet état est symbolisé dans une boîte d'état au début de la ligne. Pour modifier l'état du paquetage, cliquez dessus ou sélectionnez l'état souhaité dans le menu contextuel qui s'ouvre avec le bouton de droite de la souris. Il existe toute une série d'états, qui sont sélectionnables ou non, selon la situation globale actuelle. Par exemple, il n'est pas possible de sélectionner l'état "Supprimer" pour un paquetage qui n'est pas encore installé. Pour savoir quels sont les différents états et les symboles correspondants, sélectionnez 'Symboles' dans le menu 'Aide'.

Le gestionnaire de paquetages contient les états suivants pour les paquetages :

Ne pas installer Ce paquetage n'est pas installé et ne sera pas installé.

Installer Ce paquetage n'est pas encore installé mais va être installé.

Conserver Ce paquetage est déjà installé et ne sera pas modifié.

Actualiser Ce paquetage est déjà installé et sera remplacé par la version disponible sur le support d'installation.

Supprimer Ce paquetage est déjà installé et sera supprimé.

Tabou—ne jamais installer Ce paquetage n'est pas installé et ne sera jamais installé, quelques soient les circonstances. Il sera traité comme s'il n'existait sur aucun support d'installation. Par exemple, si un paquetage doit être ajouté automatiquement pour résoudre les dépendances, avec "Tabou", vous vous assurez qu'il ne sera pas installé. Les inconsistances qui en résultent devront alors être résolues manuellement. Pour cette raison, "Tabou" est une option destinée principalement aux experts.

Protégé Ce paquetage est installé et ne doit pas être modifié car cela pourrait provoquer des dépendances non résolues avec d'autres paquetages. Les paquetages de tiers (sans signature SUSE) se voient attribuer cet état de façon automatique pour ne pas être remplacés par des paquetages plus récents présents sur le support d'installation. Ceci pourrait provoquer des conflits entre paquetages qui devraient être résolus manuellement.

Installation automatique Le gestionnaire de paquetages a automatiquement sélectionné ce paquetage pour l'installer parce qu'il est nécessaire à un autre paquetage (résolution des dépendances entre paquetages). Pour désélectionner un de ces paquetages, il est possible que vous ayez à utiliser l'état "Tabou".

Actualisation automatique Ce paquetage est déjà installé. Cependant, il est nécessaire, dans une version plus récente, à un autre paquetage. La version installée sera donc mise à jour de façon automatique.

Suppression automatique Ce paquetage est déjà installé mais il existe un conflit entre paquetages qui rendent obligatoire la suppression de ce paquetage. Cela peut être le cas, par exemple, lorsqu'un autre paquetage remplace l'actuel.

Installation automatique (après sélection)
Ce paquetage a été sélectionné automatiquement pour être installé parce qu'il fait partie d'une sélection prédéfinie (par exemple "Multimédia" ou "Développement").

Mise à jour automatique (après sélection)
Ce paquetage est déjà installé mais il existe une version plus récente sur le support d'installation. Il fait partie d'une sélection prédéfinie (par exemple "Multimédia" ou "Développement") et est donc sélectionné et actualisé automatiquement.

Suppression automatique (après sélection)
Ce paquetage est déjà installé mais une sélection prédéfinie (par exemple "Multimédia" ou "Développement") rend sa suppression nécessaire.

En outre, il est possible de spécifier si vous souhaitez installer les sources d'un programme avec celui-ci. Cette information complète l'état du paquetage et ne peut donc être sélectionnée manuellement. À la place, une case à cocher à la fin de la ligne de description du paquetage permet la sélection des paquetages sources. Vous pouvez également trouver cette option dans le menu 'Paquetage'.

Installer les sources Le code source sera installé.

Ne pas installer les sources Le code source ne sera pas installé.

Les couleurs de caractères utilisées dans la fenêtre d'affichage individuel des paquetages apportent des informations supplémentaires. Les paquetages déjà installés qui sont disponibles dans une nouvelle version sur le support d'installation, sont affichés en bleu. Inversement, les paquetages dont la version installée est plus récente que celle présente sur le support d'installation, sont affichés en rouge. Cependant, étant donné que la numérotation des paquetages n'est pas toujours linéaire, il peut être difficile de déterminer quelle version est la plus récente. Les informations fournies ne sont donc pas absolument certaines mais suffisent généralement à indiquer les paquetages problématiques. Pour voir le numéro exact de la version, utilisez la fenêtre d'informations.

La fenêtre d'informations

En bas, à droite, vous pouvez voir la fenêtre dans laquelle sont affichées, au moyen d'onglets, différentes informations relatives au paquetage sélectionné, telles que la description détaillée qui est affichée au démarrage, les données techniques (taille, groupe, etc.), une liste d'autres paquetages dont il dépend et la version du paquetage.

La fenêtre de ressources

La fenêtre de ressources qui se trouve en bas à gauche affiche l'espace disque nécessaire à l'installation de votre sélection de paquetages courante sur les systèmes de fichiers montés pendant le processus de sélection de paquetages. L'occupation de l'espace dans chaque système de fichiers est indiqué sous forme de diagramme à barres de couleur. Le vert signifie qu'il a encore suffisamment d'espace. Plus l'espace disque diminue, plus la couleur des barres passe au rouge. Les valeurs affichées sont virtuelles et ne représentent que l'occupation d'espace qui aurait lieu si la sélection actuelle était installée. Si vous avez sélectionné trop de paquetages pour l'espace disque disponible, une fenêtre d'alerte apparaît.

La barre de menus

La barre de menus dans la partie supérieure de la fenêtre permet également d'accéder à la majorité des fonctions déjà décrites et contient les quatre menus suivants :

Fichier L'option 'Exporter' sous 'Fichier' permet de créer une liste de tous les paquetages installés et de les enregistrer dans un fichier texte. Ceci est pratique si vous souhaitez reproduire exactement la même installation à un autre moment ou sur un autre système. Avec la fonction 'Importer', vous pouvez charger un fichier créé de cette façon et générer ainsi exactement la même sélection de paquetages que celle qui a été enregistrée. Dans les deux cas, vous pouvez décider librement où enregistrer le fichier ou bien accepter la proposition du système.

L'option 'Sortir—défausser les modifications' sert à sortir du gestionnaire de paquetages en défaussant toutes les modifications qui ont été réalisées dans la sélection de paquetages depuis le démarrage du gestionnaire. Si par contre, vous sélectionnez 'Quitter—enregistrer les modifications'. Dans ce cas, les modifications sont prises en compte et le programme est fermé ensuite.

Paquetage Les options du menu 'Paquetage' s'appliquent toujours au paquetage actuellement sélectionné dans la fenêtre d'affichage individuel de paquetages. Bien que tous les états qu'un paquetage peut avoir soient indiqués, vous ne pourrez sélectionner que ceux qui sont possibles et relevants pour ce paquetage. Les cases à cocher vous permettent également d'installer les sources avec le programme. L'option 'Tous ceux de la liste' ouvre un sous-menu qui contient encore tous les états du paquetage. Cependant, un choix dans cette liste ne s'appliquera pas seulement au paquetage courant, mais à *tous* les paquetages de la liste.

Extras Le menu 'Extras' contient des options de gestion des dépendances et conflits entre paquetages. Après avoir sélectionné manuellement les paquetages pour votre installation, cliquez sur 'Afficher les changements automatiques de paquetages'. Une liste des paquetages sélectionnés automatiquement par le gestionnaire de paquetages pour résoudre les dépendances est affichée. S'il existe encore des conflits entre paquetages non résolus, une fenêtre contenant des propositions de solutions apparaît.

Lorsque vous activez l'option "Ignorer" pour les conflits entre paquetages, cette option est enregistrée de façon permanente dans le système. Sinon, vous devriez activer l'option "Ignorer" pour les mêmes paquetages lors de chaque démarrage du gestionnaire de paquetages. Pour désactiver cette option, utilisez 'Réinitialiser les conflits de dépendances ignorés'.

Aide L'option 'Aperçu' du menu 'Aide' affiche un résumé du fonctionnement du gestionnaire de paquetages. Vous trouverez une explication détaillée des états des paquetages et de leurs symboles en sélectionnant l'option 'Symboles'. Si vous souhaitez utiliser le programme sans faire appel à la souris, vous pouvez obtenir une description des combinaisons de touches à l'aide du point de menu 'Touches'.

Vérification des dépendances

Sous la fenêtre d'informations, se trouvent le bouton 'Vérifier les dépendances' et la case à cocher 'Vérification automatique'. Si vous cliquez sur le bouton 'Vérifier les dépendances', le gestionnaire de paquetages contrôle l'existence de dépendances non résolues ou de conflits dans la sélection de paquetages actuelle. En cas de dépendances non résolues, les paquetages nécessaires à la résolution des dépendances seront automatiquement sélectionnés. En cas de conflits entre paquetages, le gestionnaire de paquetages ouvre une fenêtre pour les visualiser et vous propose des possibilités de solution.

Si vous activez 'Vérification automatique', le processus de vérification décrit ci-dessus est effectué à chaque fois que l'état d'un paquetage est modifié. Ceci est pratique parce qu'ainsi les dépendances entre paquetages sont vérifiées en permanence. Cependant cela consomme des ressources et peut ralentir considérablement le fonctionnement du gestionnaire de paquetages. Pour cette raison, la vérification automatique n'est pas activée au démarrage du gestionnaire de paquetages. Vous pouvez choisir l'option qui vous semble la plus pratique. Néanmoins, la vérification des dépendances est toujours faite lorsque vous validez votre sélection en cliquant sur 'Accepter'.

Dans l'exemple suivant, les paquetages `sendmail` et `postfix` ne peuvent pas être installés simultanément. Dans la figure 2.3 page suivante, vous pouvez voir le message de conflit qui vous appelle à prendre une décision. `postfix` est déjà installé, vous pouvez donc renoncer à l'installation de `sendmail`, éliminer `postfix` ou prendre le risque d'ignorer le conflit.

Avertissement

Traitement des conflits de paquetages

Suivez les conseils de YaST pour le traitement des conflits de paquetages car cela peut affecter la stabilité et la fonctionnalité de votre système.

Avertissement

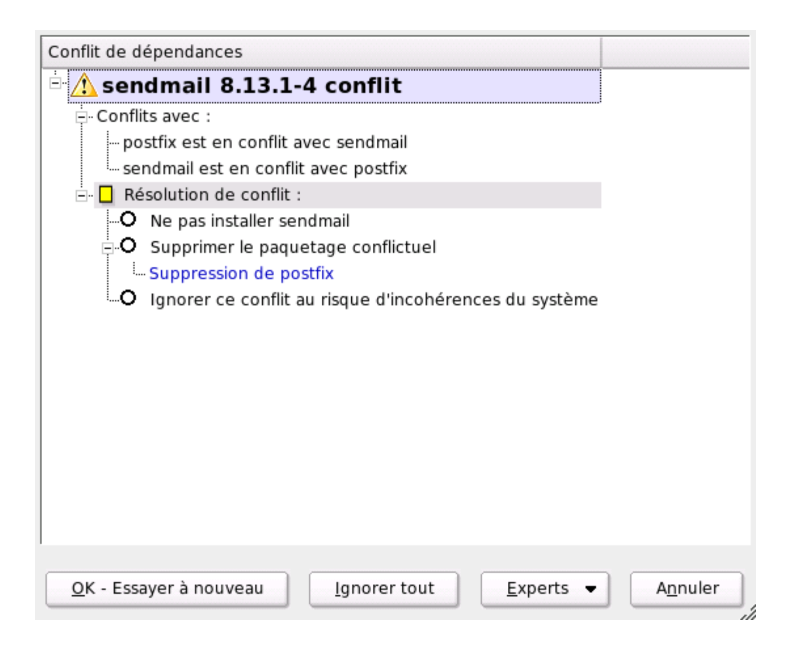


FIG. 2.3: *Gestion de conflits par le gestionnaire de paquetages*

2.2.2 Changer le support d'installation

YaST peut gérer toute une série de sources d'installation et vous permet de sélectionner celle à utiliser pour une installation ou une mise à jour. Après le démarrage du module, une liste de tous les supports d'installation enregistrés jusque là est affichée. Après une installation normale depuis un CD, cette liste ne contient que le CD comme support. Cliquez sur 'Ajouter' pour introduire de nouveaux supports d'installation. Outre des supports d'installation comme des CD et des DVD, vous pouvez également ajouter des connexions de réseau telles que serveurs NFS et FTP. Même des répertoires sur votre disque dur local peuvent également être utilisés comme supports d'installation. Consultez à ce sujet le texte d'aide relatif à YaST.

Les différents supports d'installation enregistrés peuvent être activés ou désactivés et leur état d'activation est indiqué dans la première colonne de la liste. Cliquez sur 'Activer ou Désactiver' pour changer cet état. Lors de l'installation de paquetages logiciels ou d'une mise à jour, YaST choisit l'entrée adéquate parmi

toutes les sources d'installations activées. Lorsque vous quittez le module en cliquant sur 'Fermer', la configuration actuelle est enregistrée et sera donc appliqusée aux modules de configuration 'Installer ou supprimer les logiciels' et 'Mise à jour du système'.

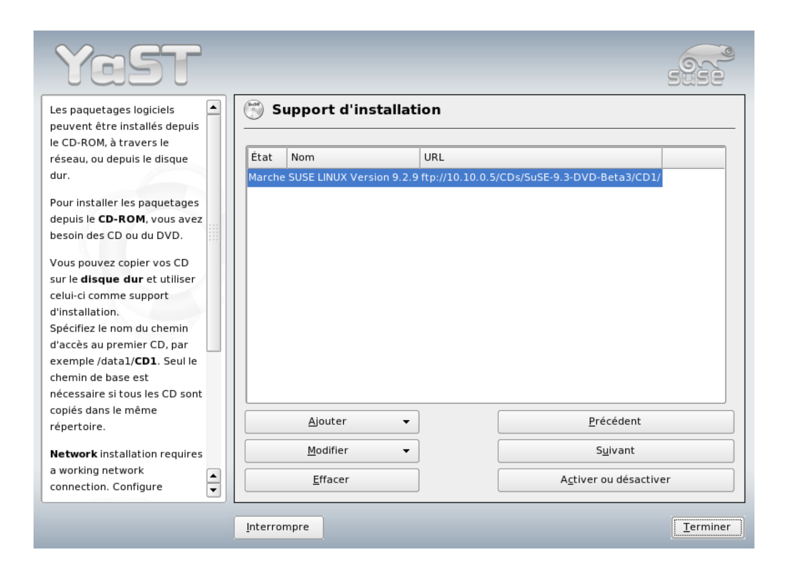


FIG. 2.4: *Changer le support d'installation*

2.2.3 YaST OnlineUpdate, Mise à jour en ligne YaST

La mise à jour en ligne YaST (YOU) permet l'installation de mises à jour importantes et autres améliorations. Ces patches sont mis à votre disposition pour téléchargement sur le serveur FTP de SUSE ainsi que sur différents serveurs miroirs.

Dans le champ 'Source d'installation', vous pouvez choisir parmi différents serveurs. Lorsque vous sélectionnez un serveur, l'URL correspondant apparaît dans le champ de texte en dessous et peut y être modifié. Vous avez également la possibilité d'introduire un URL local sous la forme "file:/mon/chemin" ou tout simplement "/mon/chemin". Cliquez sur 'Nouveau serveur' pour ajouter des nouveaux serveurs à la liste. En cliquant sur 'Modifier le serveur', vous pouvez modifier la configuration du serveur actuellement sélectionné.

Lors du démarrage du module, l'option 'Sélection manuelle des patches' est activée afin de pouvoir définir individuellement le chargement de chaque patch. Si vous souhaitez installer tous les paquetages de mises à jour sans distinction, désactivez cette option. Selon la largeur de bande de la connexion et la quantité de données à télécharger, le temps de chargement peut être très long.

Si vous activez la case à cocher 'Charger à nouveau tous les patches', *tous* les patches, paquetages installables et descriptions disponibles sur le serveur seront téléchargés. Si elle n'est pas activée (configuration par défaut), vous ne téléchargerez que les paquetages qui ne sont pas encore installés sur votre système.

En outre, vous avez la possibilité de maintenir le système actualisé en permanence automatiquement. Avec l'option 'Configurer la mise à jour totalement automatique', vous définissez un processus qui recherche régulièrement les nouvelles mises à jour et les applique. Ce processus est totalement automatisé. Il est simplement nécessaire qu'une connexion au serveur de mises à jour soit établie au moment prévu pour la mise à jour.

Pour procéder à la mise à jour, cliquez sur 'Suivant'. Dans le cas d'une mise à jour manuelle, ceci charge une liste de tous les patches disponibles puis démarre le gestionnaire de paquetages tel que décrit dans la section 2.2.1 page 39. Le filtre pour les patches YOU est alors automatiquement activé et il vous est possible de déterminer les mises à jour que vous souhaitez installer. Les patches de sécurité et les patches recommandés sont déjà présélectionnés lors du démarrage si les paquetages correspondants sont installés dans le système. Il est préférable d'accepter cette présélection.

Une fois que vous avez sélectionné les patches, cliquez, dans le gestionnaire de paquetages, sur 'Accepter'. Tous les patches sélectionnés sont alors téléchargés depuis le serveur puis sont installés sur l'ordinateur. Selon la qualité de la connexion et les performances de votre ordinateur, ce processus peut durer. Les erreurs possibles sont affichées dans une fenêtre et, le cas échéant, vous pourrez ignorer le paquetage qui pose problème. Certains patches ouvrent une fenêtre avant l'installation pour afficher des informations détaillées.

Lors du téléchargement et de l'installation des mises à jour, vous pouvez suivre le processus dans la fenêtre de protocole. Quittez le dialogue de YOU avec 'Terminer', une fois que vous aurez terminé l'installation de tous les patches. Si vous ne voulez pas conserver les patches une fois la mise à jour effectuée, cliquez sur 'Effacer les sources après la mise à jour'. Le programme SuSEconfig sera alors exécuté afin d'adapter la configuration de votre système aux nouvelles conditions.

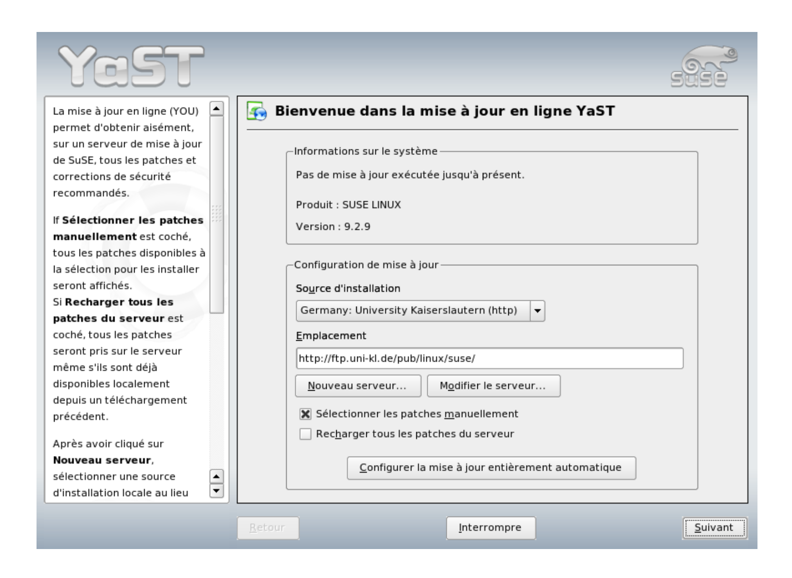


FIG. 2.5: *YaST~: Mise à jour en ligne*

2.2.4 Mise à jour depuis le CD de patches

Avec cette option, lles patches ne sont pas téléchargés depuis le serveur ftp mais chargés directement depuis le CD-ROM. La mise à jour depuis le CD-ROM présente l'avantage d'être plus rapide. Une fois que le CD de patches a été inséré, tous les patches qui s'y trouvent seront lus et affichés dans le dialogue. Dans cette liste de patches, vous pouvez sélectionner lesquels devront être installés. Si vous avez oublié d'introduire le CD-ROM, un message d'erreur vous en avertira. Insérez alors le CD-ROM et redémarrez le module.

2.2.5 Mise à jour du système

Ce module vous permet d'actualiser votre système. Si votre système est en fonctionnement, vous ne pourrez mettre à jour que les logiciels d'applications mais pas le système de base SUSE LINUX. À cette fin, vous devez amorcer depuis le support d'installation, par exemple à partir du CD. Lors de la sélection du mode d'installation dans YaST, sélectionnez 'Mise à jour du système installé' au lieu de 'Nouvelle installation'.

Le processus de mise à jour ressemble beaucoup à une nouvelle installation du système. YaST vérifie tout d'abord l'état actuel de votre système, détermine une stratégie de mise à jour appropriée et présente les résultats dans un dialogue de propositions. Vous pouvez sélectionner les différentes options à l'aide de la souris pour procéder à des modifications individuelles. La majorité des options telles que 'Langue' et 'Disposition du clavier' ont déjà été expliquées dans la section traitant de l'installation (voir la section 1.3 page 8). En conséquence, nous nous en tiendrons ici à vous expliquer les éléments spécifiques à la mise à jour.

Sélectionné pour la mise à jour

Si différentes versions de SUSE LINUX sont installées sur votre système, vous pouvez sélectionner ici la partition que vous souhaitez mettre à jour. La liste affiche toutes les partitions qui peuvent être actualisés.

Options de mise à jour

Sélectionnez la méthode de mise à jour de votre système. Vous disposez de deux possibilités différentes.

Mise à jour avec installation de nouveaux logiciels
: Si vous souhaitez mettre à jour tout le système, vous pouvez choisir l'une des sélections prédéfinis. Ces sélections sont les mêmes que celles offertes lors de l'installation et permettent également l'installation de nouveaux paquetages.

Mise à jour des paquetages installés uniquement
: Avec cette option, uniquement les paquetages déjà installés sur le système seront mis à jour. Aucun nouveau logiciel ne sera installé.

Vous pouvez également, avec l'option 'Supprimer les paquetages obsolètes', spécifier si les paquetages qui ne sont pas disponibles dans la nouvelle version doivent être effacés. Cette option est sélectionnée par défaut pour éviter que les paquetages obsolètes n'occupent de l'espace disque inutilement.

Paquetages

En cliquant sur 'Paquetages', vous démarrez le gestionnaire de paquetages et vous pourrez y sélectionner ou désélectionner individuellement les paquetages pour la mise à jour. Les conflits entre paquetages qui peuvent apparaître pourront y être résolus à l'aide de la vérification des dépendances. L'utilisation du gestionnaire de paquetages a été expliquée en détails dans la section 2.2.1 page 39.

Sauvegarde

Lors de la mise à jour du système, il est possible que les fichiers de configuration de certains paquetages soient remplacés par ceux de la nouvelle version. Étant donné que vous pouvez avoir modifié ces fichiers dans votre système actuel (avant mise à jour), par conséquent, ceux-ci sont sauvegardés avant la mise à jour. Ce dialogue vous permet de déterminer si ces sauvegardes doivent être effectuées et quelle doit être leur importance.

Important

Contenu de la sauvegarde

Veuillez noter que ces sauvegardes ne concernent pas le logiciel mais les fichiers de configuration correspondants.

Important

Informations importantes au sujet de la mise à jour

La mise à jour d'un système est, d'un point de vue technique, une opération extrêmement complexe. À cette occasion, YaST doit, pour chaque paquetage logiciel, vérifier quelle version est installée puis définir ce qui doit être fait afin que la nouvelle version remplace correctement l'ancienne. YaST s'assure de reprendre, dans la mesure du possible, pour chaque paquetage installé concerné, les configurations personnelles existantes afin de vous éviter de reconfigurer vos paramètres à chaque fois. Dans certains cas, certains problèmes de configuration peuvent se présenter après la mise à jour si l'ancienne configuration n'est pas compatible avec la nouvelle version du programme ou parce qu'il y a une inconsistance imprévisible entre différentes configurations.

En outre, une mise à jour pose d'autant plus de problèmes que la version à actualiser est ancienne. Des difficultés sont aussi à prévoir si la configuration des paquetages à actualiser s'éloigne du standard. Il est parfois impossible de reprendre correctement une ancienne configuration et il est alors nécessaire d'en créer une nouvelle. Une configuration existante devrait toujours être sauvegardée avant le début de la mise à jour.

2.2.6 Vérification des supports

Si vous rencontrez des problèmes avec les supports d'installation de SUSE LINUX, vous pouvez vérifier les CD ou DVD à l'aide de ce module. Dans de rares

cas, certains périphériques peuvent avoir des problèmes de lecture avec certains supports. Cela a plus de chance d'arriver avec des supports "faits maison". Pour vérifier qu'un CD ou DVD SUSE LINUX ne comporte pas d'erreurs, insérez le support dans le lecteur et exécutez ce module. Cliquez sur 'Démarrer' et YaST vérifie la somme de contrôle MD5 du support. Cela peut prendre plusieurs minutes. Si des erreurs sont détectés, n'utilisez pas ce support pour l'installation.

2.3 Matériel

Les nouveaux composants matériels doivent tout d'abord être intégrés ou connectés selon les instructions fournies par le constructeur. Activez les périphériques externes tels que l'imprimante ou le modem et lancez le module YaST correspondant. Les composants matériels que l'on trouve habituellement dans le commerce sont, pour la plupart, reconnus automatiquement par YaST qui affiche ensuite leurs données techniques. Si la détection automatique se solde par un échec, YaST vous présentera une liste (par exemple, noms de modèles/constructeurs) dans laquelle vous pourrez sélectionner le périphérique adéquat. Consultez la documentation relative à votre matériel si les informations inscrites sur votre périphérique ne sont pas suffisantes.

Important

Noms de modèles

Si votre modèle ne figure pas dans la liste, vous pouvez toujours faire un essai en sélectionnant un nom similaire. Dans certains cas, il est cependant indispensable de spécifier le nom exact en tenant compte de chaque lettre ou numéro car un nom similaire ne permet pas toujours de conclure qu'il s'agit d'un périphérique compatible.

Important

2.3.1 Lecteurs CD et DVD

Lors de l'installation, tous les lecteurs de CD-ROM détectés sont intégrés au système, c'est à dire que les entrées correspondantes seront faites dans le fichier `/etc/fstab` et les sous-répertoires `/media` seront créés. Avec ce module de YaST, vous pouvez également intégrer au système des unités montées ultérieurement.

Une fois que le module est démarré, une liste contenant toutes les unités détectées est affichée. Sélectionnez le nouveau lecteur en cochant la case au début de la ligne, puis cliquez sur 'Terminer'. Le nouveau lecteur est maintenant intégré au système et peut être utilisé.

2.3.2 Imprimante

Vous trouverez des informations plus détaillées relatives à l'impression sous Linux au chapitre 12 page 261 qui traite de l'impression en général. YaST permet de configurer automatiquement l'imprimante ou offre des dialogues de configuration qui apportent une aide pour configurer manuellement l'imprimante. Vous pouvez alors imprimer depuis la ligne de commande ou configurer des applications pour utiliser le système d'impression. Vous trouverez une description détaillée de la configuration des imprimantes avec YaST à la section 12.5.1 page 266.

2.3.3 Contrôleur de disques durs

Normalement, YaST configure le contrôleur de disques durs de votre système durant l'installation. Si vous montez des contrôleurs supplémentaires, vous pouvez procéder à leur intégration dans le système avec ce module de YaST. Vous pouvez également modifier la configuration existante, ce qui, cependant, ne devrait pas être nécessaire.

La fenêtre de dialogue offre une liste de tous les contrôleurs de disques durs détectés et permet d'ordonner les modules de noyau adéquats avec des paramètres spécifiques. Utilisez 'Tester le chargement du module' pour vérifier si les configurations actuelles fonctionnent avant de les enregistrer définitivement dans le système.

Avertissement

Configuration du contrôleur de disques durs

Ceci est un outil pour experts. Si vous faites ici à une mauvaise configuration, il se peut que le système ne puisse plus amorcer. Si vous procédez à des modifications, utilisez l'option de test.

Avertissement

2.3.4 Informations sur le matériel

Pour la configuration des composants matériels, YaST procède à une reconnaissance du matériel. Les données techniques détectées sont affichées dans une fenêtre propre. Ceci est particulièrement utile lorsque vous souhaitez soumettre une requête à notre service d'assistance technique. Pour cela, vous nécessitez des informations sur votre matériel.

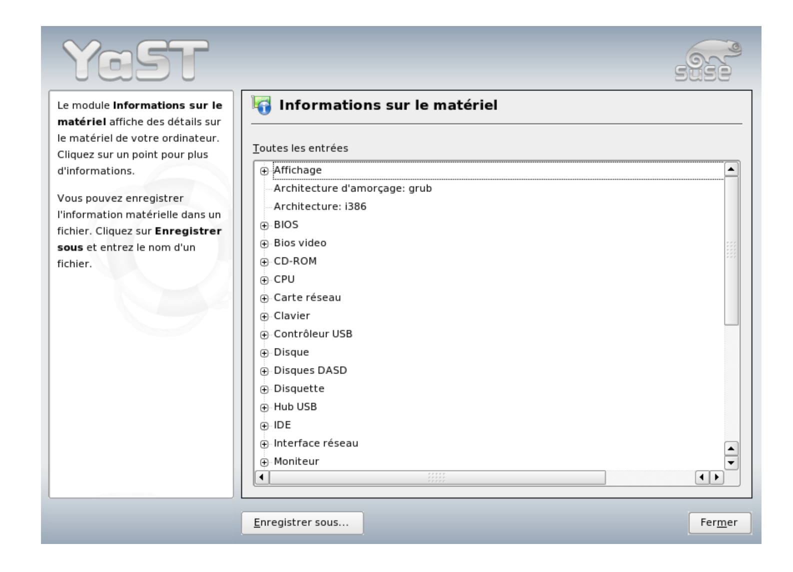


FIG. 2.6: *Affichage des informations sur le matériel*

2.3.5 Mode IDE DMA

Ce module vous permet d'activer ou de désactiver le mode DMA pour le(s) disque(s) dur(s) (IDE) et le(s) lecteur(s) de CD/DVD (IDE) dans le système installé. Ce module ne fonctionne pas pour les périphériques SCSI. Les modes DMA peuvent accroître sensiblement la performance ou la vitesse de transfert de données de votre système.

Lors de l'installation du système, le noyau actuel de SUSE LINUX active automatiquement DMA pour les disques durs et le désactive pour les lecteurs de CD car ceux-ci ont très souvent créé des problèmes lorsque DMA est activé pour tous les lecteurs. Vous pourrez ensuite décider, avec le module DMA, d'activer ou non

ce mode pour vos lecteurs. En cas de problèmes, par exemple, dans le fonctionnement de votre disque dur, il peut être utile de désactiver DMA. Inversement, vous pouvez améliorer le taux de transfert de données de votre lecteur de CD en activant DMA si le lecteur supporte ce mode sans problème.

Important

DMA (direct memory access) signifie qu'il y a un accès direct à la memoire, c'est à dire que les lecteurs peuvent transférer vos données directement dans la mémoire de travail sans qu'il soit nécessaire de faire un détour par le processeur.

Important

2.3.6 Scanneur

Si vous avez connecté et activé votre scanneur, celui-ci devrait être reconnu automatiquement au lancement de ce module de YaST. Vous verrez alors apparaître le dialogue d'installation du scanneur. Si aucun scanneur n'a été détecté, la procédure se poursuivra avec la configuration manuelle. Si vous avez déjà installé un ou plusieurs scanneurs, vous verrez s'afficher un tableau synoptique avec une liste des scanneurs présents que vous pourrez modifier ou supprimer. Avec 'Ajouter', vous pourrez intégrer un nouveau scanneur.

Il sera ensuite effectué une installation avec des paramètres standards. Si le processus d'installation a abouti, vous en serez informé par un message. Vous aurez alors la possibilité de tester votre scanneur en plaçant un document sur celui-ci et en cliquant sur 'Tester'.

Le scanneur n'a pas été détecté

Tenez présent à l'esprit que seuls les scanneurs supportés peuvent être détectés automatiquement. Les scanneurs utilisés sur une autre machine connectée au réseau ne sont pas reconnus non plus. Il convient, lors de la configuration manuelle, de faire une distinction entre les scanneurs USB, les scanneurs SCSI et les scanneurs réseau.

Scanneur USB Vous devez ici spécifier le nom du constructeur ou du modèle. YaST tente de charger des modules USB. Si vous possédez un scanneur très récent, il est possible que les modules ne puissent pas être chargés automatiquement. Dans ce cas, vous arriverez à un dialogue qui vous donne la possibilité de charger à la main le module USB. Lisez à ce sujet le texte d'aide de YaST.

Scanneur SCSI Spécifiez le nom du périphérique, par exemple, `/dev/sg0`. Veuillez noter qu'un scanneur SCSI ne doit pas être connecté ou déconnecté lorsque le système est en fonctionnement. Arrêtez tout d'abord votre système.

Scanneur réseau Il vous faut ici l'adresse IP ou le nom d'hôte. Pour la configuration d'un scanneur en réseau, lisez l'article de la base de données support *Scanning in Linux* (`http://portal.suse.com/sdb/en/index.html`, mot clé *scanner*).

Si votre scanneur n'a pas été détecté, il est probable qu'il ne soit pas supporté. Il peut cependant arriver que même des scanneurs supportés ne soient pas détectés. Dans un tel cas, vous pourrez aussi avoir recours à la sélection manuelle du scanneur. Si vous pouvez identifier votre scanneur dans la liste des constructeurs et des modèles, sélectionnez-le tout simplement. Sinon, cliquez sur 'Annuler'. Vous trouverez des informations sur les scanneurs fonctionnant avec Linux sous `http://cdb.suse.de/` et `http://www.mostang.com/sane`.

Avertissement

Assignation manuelle du scanneur

Ne procédez à l'assignation manuelle du scanneur que si vous êtes sûr de ne commettre aucune erreur. Une sélection inappropriée risque d'endommager votre matériel.

Avertissement

Dépannage

Si votre scanneur n'a pas été détecté, ceci peut être dû aux causes suivantes :

- Le scanneur n'est pas supporté. Sous `http://cdb.suse.de/`, vous trouverez une liste des périphériques compatibles avec Linux.
- Le contrôleur SCSI n'est pas correctement installé.
- Il y a des problèmes de terminaison avec votre port SCSI.
- La longueur du câble SCSI dépasse la limite admise.
- Le scanneur est doté d'un contrôleur Light SCSI qui n'est pas supporté par Linux.
- Le scanneur est défectueux.

Avertissement

Un scanneur SCSI ne doit en aucun cas être connecté ou déconnecté pendant le fonctionnement du système. Arrêtez d'abord votre système.

Avertissement

Vous trouverez des informations plus détaillées sur la numérisation et les scanneurs dans le *Guide de l'utilisateur* au chapitre `kooka`.

2.3.7 Son

Au lancement du module de configuration du son, YaST tente de détecter automatiquement votre carte son. Si vous le souhaitez, vous pouvez configurer une ou plusieurs cartes son. Si vous souhaitez configurer plusieurs cartes, sélectionnez tout d'abord l'une des cartes que vous voulez utiliser. Avec le bouton 'Configurer', vous arriverez au menu 'Configuration'. Avec le bouton 'Modifier', vous pourrez, sous 'Configuration du son', modifier les paramètres d'une carte déjà configurée. Un clic sur le bouton 'Terminer' enregistre votre configuration actuelle et achève le processus de configuration du son.

Dans le cas où YaST ne reconnaîtrait pas automatiquement votre carte son, vous pouvez, dans le menu 'Configuration du son', cliquer sur 'Ajouter une carte son' pour ouvrir un dialogue dans lequel sélectionner un carte son et le module adéquat. Consultez, la documentation de votre carte son pour obtenir les informations nécessaires. Vous pourrez également trouver une liste des cartes supportées par ALSA avec le module son correspondant à chaque carte sous `/usr/share/doc/packages/alsa/cards.txt` et `http://www.alsa-project.org/~goemon/`. Après avoir fait votre sélection, vous reviendrez au menu 'Configuration' en cliquant sur 'Suivant'.

Configuration

Choisissez le niveau de configuration dans le premier écran de configuration. Avec 'Configuration automatique rapide', vous n'aurez pas à parcourir d'autres étapes de configuration et il ne sera pas effectué de test sonore. La configuration de votre carte son faite automatiquement. Avec 'Configuration normale', vous avez la possibilité de régler le volume de sortie et de lire un échantillon sonore. 'Configuration avancée' vous permet de modifier manuellement les options des modules son.

En outre, vous pouvez ici configurer votre joystick, en cliquant sur la case à cocher du même nom. Dans le dialogue qui apparaît, sélectionnez le modèle de votre joystick puis cliquez sur 'Suivant'.

Volume de la carte son

Dans ce masque, vous pouvez tester la configuration de votre carte son. Avec les boutons '+' et '-', vous pouvez régler le volume sonore. Nous vous conseillons de commencer à environ 10% pour ne pas endommager vos haut-parleurs et ne faire courir aucun risque à vos oreilles. Après avoir cliqué sur le bouton 'Tester', vous devriez entendre un échantillon sonore. Si vous n'entendez rien, ajustez le volume. En cliquant sur 'Suivant', vous terminez la configuration du son et enregistrez les paramètres du volume.

Configuration du son

Avec l'option 'Supprimer', vous pouvez éliminer une carte son. Les entrées concernant les cartes son déjà configurées sont désactivées dans le fichier `/etc/modprobe.d/sound`. Sous 'Options', vous accédez à un dialogue qui vous permet d'adapter manuellement les options des modules son. Avec 'Ajouter la carte son', vous pouvez intégrer des cartes son supplémentaires. Si YaST détecte automatiquement une autre carte son, vous arriverez au menu 'Configurer une carte son'. Si YaST ne trouve pas de carte son, vous passerez directement à l'option 'Sélection manuelle de la carte son'.

Si vous utilisez une carte `Creative Soundblaster Live` ou `AWE`, vous pouvez, à l'aide de l'option 'Installer des fontes sonores', copier sur votre disque dur des fontes sonores SF2 provenant du CD-ROM pilote Soundblaster original. Ces fontes seront enregistrées dans le répertoire `/usr/share/sfbank/creative/`.

Pour lire des fichiers Midi, vous devez avoir activé la case à cocher 'Démarrer le séquenceur'. Les modules pour le support du séquenceur seront alors chargés en même temps que les modules son.

En activant 'Terminer', vous enregistrez les paramètres pour le volume et la configuration de toutes les cartes installées jusqu'à présent. Les paramètres concernant le mixer sont insérés dans le fichier `/etc/asound.conf` et les données de configuration ALSA sont ajoutées à la fin du fichier `/etc/modprobe.conf`

2.3.8 Cartes TV et radio

Après le démarrage et l'initialisation de ce module de YaST, vous voyez tout d'abord apparaître le dialogue 'Cartes TV et radio'. Si votre carte a été reconnue automatiquement, elle apparaîtra en haut de la liste. Sélectionnez la ligne correspondante par un clic de souris et cliquez ensuite sur 'Configurer'. Dans le cas où

votre carte n'aurait pas été reconnue, sélectionnez 'Autre (non reconnue)'. Cliquez sur 'Configurer' pour accéder à la sélection manuelle et sélectionner votre carte dans la liste des modèles et fabricants.

Si vous avez déjà configuré des cartes TV ou radio, le bouton 'Modifier' vous donne la possibilité d'apporter des changements à cette configuration. Dans ce cas, un dialogue qui contient une liste de toutes les cartes configurées s'ouvre. Sélectionnez une carte et démarrez la configuration manuelle avec 'Modifier'.

Lors de la détection automatique du matériel, YaST tente d'assigner le tuner correct à votre carte. Si vous avez un doute, choisissez 'Par défaut (détecté)' et vérifiez si cela fonctionne. Si vous n'avez pas pu sélectionner tous les émetteurs, cela peut être du, par exemple, au fait que la reconnaissance automatique du type de tuner a échoué. Dans ce cas, cliquez sur le bouton 'Sélectionner le tuner' et choisissez le type de tuner approprié dans la liste de sélection.

Si vous êtes familiarisé aux spécifications techniques, vous pouvez procéder à une configuration plus fine de votre carte TV ou radio dans le dialogue pour experts. Vous pouvez y sélectionner spécifiquement un module noyau et ses paramètres. Vous pouvez également contrôler tous les paramètres du pilote de la carte TV. Pour cela, sélectionnez les paramètres à modifier et entrez les nouvelles valeurs dans les lignes correspondantes. Confirmez les nouvelles valeurs en cliquant sur 'Appliquer' ou restaurez les valeurs par défaut avec 'Réinitialiser'.

Dans le dialogue 'Cartes TV et radio, audio', vous pouvez connecter la carte TV ou radio avec la carte son installée. Outre dans leur configuration, les cartes doivent également être connectées par un câble qui relie la sortie de la carte TV ou radio avec l'entrée audio externe de la carte son. Pour cela, la carte son doit déjà être configurée et l'entrée externe doit être activée. Si vous n'avez pas encore configuré votre carte son, faites-le dans le dialogue correspondant avec 'Configurer la carte son' (voir la section 2.3.7 page 60).

Si la carte TV ou radio dispose de fiches pour haut-parleurs, vous pouvez les connecter directement et il ne sera pas nécessaire de configurer la carte son. Il existe également des cartes TV sans fonction audio, celles pour caméras CCD par exemple, qui ne nécessitent donc pas de configuration du son non plus.

2.4 Périphériques réseau

Tous les périphériques réseau du système doivent être initialisés avant de pouvoir être utilisés par un service. La détection et la configuration de ces périphériques se fait dans le groupe de modules 'Périphériques réseau'. Vous trouverez

une description détaillée de la configuration YaST de tous types de périphériques réseau supportés ainsi que des informations sur la connexion au réseau dans la section 22.4 page 433. La configuration de périphériques réseau pour la communication sans fil est décrite dans le chapitre 17 page 347.

2.5 Services réseau

Vous trouverez dans ce groupe des outils destinés à la configuration de tous types de services de réseau. Ces services comprennent la résolution de noms, l'authentification des utilisateurs et les services de fichiers.

2.5.1 Agent de transfert de message (MTA)

Le module de configuration vous permet de configurer vos options de courrier si vous utilisez les programmes sendmail ou postfix, ou si vous envoyez vos messages à travers le serveur SMTP de votre fournisseur. Vous pouvez télécharger les messages qui vous sont destinés à l'aide de SMTP ou avec le programme fetchmail, dans lequel vous devez spécifier les données des serveurs POP3 ou IMAP de votre fournisseur. Vous pouvez également utiliser le programme de messagerie de votre choix, par exemple KMail ou Evolution, pour spécifier vos données d'accès POP et SMTP comme à votre habitude (réception avec POP3, envoi avec SMTP). Dans ce cas, vous n'avez pas besoin de ce module.

Si vous souhaitez procéder à la configuration de votre courrier électronique avec YaST, le système vous demandera dans la première fenêtre du dialogue, les données du type de connexion désirée pour accéder à Internet. Vous disposez des options suivantes :

'Permanente' Si vous souhaitez une connexion permanente avec Internet, sélectionnez cette option. Votre ordinateur sera en ligne sans interruption et aucune numérotation supplémentaire ne sera nécessaire. Si votre système se trouve dans un réseau local avec un serveur central de messagerie électronique pour l'envoi des messages, sélectionnez également cette option pour garantir un accès permanent à votre courrier.

'Composition' Cette option de menu est utile pour tous les utilisateurs qui ont à la maison un ordinateur connecté à aucun réseau et qui doivent se connecter de temps en temps pour accéder à Internet.

Sans connexion Si vous ne disposez d'aucune connexion à Internet et vous n'appartenez à aucun réseau, vous ne pourrez ni envoyer ni recevoir de courrier électronique.

En outre, vous pouvez lancer l'antivirus pour les messages entrants en activant la case à cocher de AMaViS. Le paquetage correspondant sera installé automatiquement dès que vous activerez le filtre de courrier. Dans le dialogue suivant, spécifiez le serveur de courrier sortant (le serveur SMTP de votre fournisseur) et les paramètres pour le courrier entrant. Si vous utilisez une connexion téléphonique (dial-up), vous pouvez indiquer divers serveurs POP ou IMAP pour la réception du courrier par différents utilisateurs. Enfin, vous pouvez, de façon optionnelle, ajouter des alias supplémentaires, configurer le masquage ou définir des domaines virtuels dans ce dialogue. Quittez la configuration du courrier en cliquant sur 'Terminer'.

2.5.2 Autres services disponibles

De nombreux autres modules réseau sont disponibles dans YaST.

Serveur DHCP À l'aide de YaST, vous pouvez, en quelques étapes, configurer votre propre serveur DHCP. Vous trouverez des informations à ce sujet ainsi qu'une description des différentes étapes de la configuration avec YaST dans le chapitre 27 page 499.

Serveur DNS Dans le réseaux de grande taille, il est conseillé de configurer un serveur DNS qui prendra en charge la résolution de noms pour ce réseau. Sa configuration à l'aide de YaST est décrite dans la section 24.1 page 464. Le chapitre 24 page 463 contient des informations relatives au service DNS.

DNS et nom d'hôte Ce module sert à la configuration du nom d'hôte et de DNS lorsque celle-ci n'a pas été faite lors de la configuration du périphérique réseau. Il est également intéressant pour modifier le nom de l'ordinateur et du domaine. Si vous avez configuré correctement l'accès DSL, modem ou RNIS de votre fournisseur, vous verrez ici, dans la liste du serveur de noms, des entrées qui ont été faites automatiquement étant donné qu'elles ont été obtenues à partir des données du fournisseur d'accès. Si vous vous trouvez dans un réseau local, vous obtiendrez probablement le nom d'hôte via DHCP. Dans ce cas, veillez à ne pas changer le nom.

Serveur HTTP Si vous souhaitez avoir votre propre serveur web, configurez Apache à l'aide de YaST. Vous trouverez plus d'informations à ce sujet dans le chapitre 30 page 543.

Noms d'hôte À l'amorçage et dans les petits réseaux, la résolution de nom d'hôte peut également être faite à l'aide de ce module au lieu d'utiliser DNS. Les entrées dans ce module correspondent aux données dans le fichier `/etc/hosts`. Pour plus d'informations, veuillez consulter la section /etc/hosts page 450.

Client LDAP Outre NIS, vous disposez également de LDAP pour procéder à l'authentification des utilisateurs dans le réseau. Vous trouverez des informations relatives à LDAP ainsi qu'une description détaillée de la configuration d'un client avec YaST dans le chapitre 29 page 517.

Client NFS et serveur NFS NFS vous donne la possibilité de gérer un serveur de fichiers auquel tous les membres de votre réseau peuvent accéder. Sur ce serveur de fichiers, vous pouvez mettre certainses applications, des données et même de la mémoire à disposition des utilisateurs. Dans le module 'Serveur NFS', vous pouvez configurer votre ordinateur en tant que serveur NFS et déterminez quels répertoires doivent être pour être utilisés par les utilisateurs du réseau. Chaque utilisateur à qui le droit a été accordé peut alors monter ces répertoires dans sa propre arborescence. Vous trouverez la description de ce module YaST et des informations relatives à NFS dans le chapitre 26 page 491.

Client NIS et Serveur NIS Dès que vous utilisez plus d'un système, l'administration des utilisateurs (à l'aide des fichiers `/etc/passwd` et `/etc/shadow`) devient pénible et nécessite une maintenance importante. Dans de tels cas, les données des utilisateurs devraient être administrés sur un serveur central et, à partir de celui-ci, être déployées sur les clients. Outre LDAP et Samba, vous disposez également de NIS. Vous trouverez des informations détaillées sur NIS et sa configuration avec YaST dans le chapitre 25 page 485.

Client NTP NTP (Network Time Protocol) est un protocole utilisé pour la synchronisation de l'horloge d'un ordinateur via un réseau. Vous trouverez des informations relatives à NTP et la description de sa configuration avec YaST dans le chapitre 28 page 509.

Services réseau (inetd) Avec cet outil, vous pouvez définir quels services système (par exemple, finger, talk et ftp) doivent être démarrés lors de l'amorçage de SUSE LINUX. Ainsi, d'autres hôtes externes peuvent se connecter à votre ordinateur à travers ces services. Différents paramètres peuvent être définis pour chaque service. Par défaut, le service de niveau supérieur qui gère les différents services réseaux (inetd ou xinetd) n'est pas démarré.

Au démarrage de ce module, sélectionnez lequel des deux services inetd ou xinetd doit être démarrés. Le démon sélectionné peut être démarré avec une

sélection standard de services réseau ou avec une sélection personnalisée de services réseau dans laquelle vous pouvez 'Ajouter' de nouveaux services ou 'Supprimer' ou 'Modifier' des services existants.

Avertissement

Configuration des services réseau (inetd)

La mise en place et l'organisation de services de réseau sur un système est un processus complexe qui requiert des connaissances très précises du concept des services Linux.

Avertissement

Proxy Ce module vous permet de modifier les paramètres des proxy pour tout le système. Vous trouverez des informations détaillées sur les proxy dans le chapitre 33 page 605.

Administration depuis un ordinateur distant
Si vous souhaitez maintenir votre système à travers une connexion VNC depuis un ordinateur distant, autorisez l'établissement de la connexion avec ce module YaST. Consultez la section 3.2.2 page 95.

Routage Vous n'avez besoin de cet outil que si vous vous connectez à Internet au moyen d'une passerelle dans le réseau local. Pour une connexion DSL, les données de la passerelle sont nécessaires uniquement pour activer les cartes réseau. Néanmoins, les entrées faites pour DSL ne sont que des valeurs fictives sans aucune fonction.

Configuration de serveurs et clients Samba
Si vous souhaitez utiliser un réseau hétérogène avec des machines Linux et des machines Windows, Samba gère la communication entre le deux mondes. Vous trouverez des informations détaillées relatives à Samba et à la configuration des clients et serveurs dans le chapitre 32 page 591.

2.6 Sécurité et utilisateurs

L'une des propriétés fondamentales de Linux est sa fonctionnalité multiutilisateur qui permet à plusieurs personnes de travailler simultanément mais de manière indépendante sur un seul et même système Linux. Chacun possède son propre compte utilisateur constitué par un nom d'utilisateur ou nom de login et par un mot de passe personnel qui lui permettent de se connecter au système. Chacun a son répertoire personnel dans lequel il stocke ses fichiers privés et enregistre ses configurations.

2.6.1 Gestion des utilisateurs

Après avoir lancé cet outil, YaST met à votre disposition une liste de tous les utilisateurs locaux qui ont accès au système. Si vous vous trouvez dans un grand réseau, vous pouvez utiliser l'option 'Créer un filtre' pour générer une liste de tous les utilisateurs du système (par exemple, `root`) ou des utilisateurs NIS. Vous avez aussi la possibilité de créer des filtres personnalisés. Au lieu de passer d'un groupe d'utilisateurs à un autre, combinez-les à votre convenance. Pour ajouter des utilisateurs, remplissez les champs correspondants dans le masque suivant. Le nouvel utilisateur pourra ensuite se connecter à l'ordinateur avec son nom de login et son mot de passe. L'option 'Détails' vous permet de procéder à une configuration plus détaillée du profil de l'utilisateur. Il est possible de configurer manuellement l'ID utilisateur le répertoire personnel et le shell de connexion par défaut. En outre, il est possible d'assigner l'utilisateur à des groupes déterminés. La période de validité du mot de passe se configure dans 'Configuration du mot de passe'. Tous les paramètres peuvent être modifiés en cliquant sur le bouton 'Modifier'. Pour éliminer un utilisateur, sélectionnez-le dans la liste et cliquez sur 'Supprimer'.

Pour l'administration avancée du réseau, vous avez la possibilité de spécifier les options par défaut pour la création de nouveaux utilisateurs dans 'Options pour experts'. Vous définissez le type d'authentification (NIS, LDAP, Kerberos ou Samba) ainsi que l'algorithme utilisé pour le chiffrement du mot de passe. Ces options de configuration sont surtout intéressantes pour les grands réseaux.

2.6.2 Gestion des groupes

Démarrez le module de gestion des groupes du centre de contrôle de YaST ou cliquez sur la case à cocher 'Groupes' dans la gestion des utilisateurs. La fonctionnalité des deux masques est identique, permettant la création, la modification et la suppression de groupes.

Pour faciliter la gestion des groupes, YaST met à votre disposition une liste de tous les groupes. Pour éliminer un groupe, cliquez dans la liste sur la ligne correspondante afin que celle-ci apparaisse en bleu foncé puis cliquez sur 'Supprimer'. Pour 'Ajouter' et 'Modifier' un groupe, entrez, dans le masque correspondant de YaST, les nom, ID de groupe (gid) et utilisateurs de ce groupe. Si vous le souhaitez, vous pouvez également attribuer un mot de passe pour l'entrée dans ce groupe. Les paramètres pour le filtre sont identiques au dialogue 'Gestion des utilisateurs'.

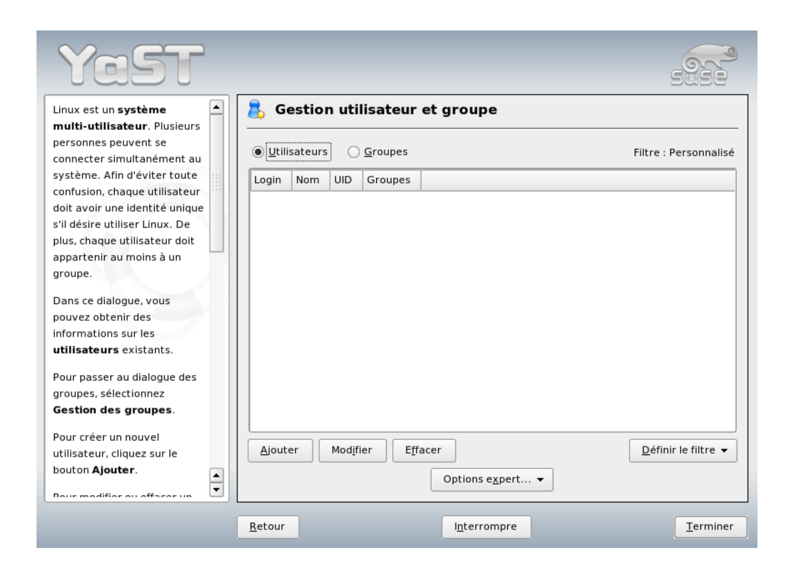


FIG. 2.7: *Gestion des utilisateurs*

2.6.3 Paramètres de sécurité

Le dialogue de démarrage intitulé 'Configuration de la sécurité locale' que vous pouvez invoquer sous 'Sécurité et utilisateurs', vous donne le choix entre quatre options : le 'niveau 1' est pour les machines monopostes (préconfiguré), le 'niveau 2' est pour les stations de travail en réseau (préconfiguré), le 'niveau 3' est pour les serveurs en réseau (préconfiguré) et la configuration 'personnalisée' est pour vos propres paramètres.

Si vous avez sélectionné l'une des trois premières options, vous avez la possibilité d'utiliser, pour la sécurité du système, une configuration déjà prédéfinie. Cliquez simplement sur 'Terminer'. Sous 'Détails', vous avez accès aux différentes configurations que vous pouvez modifier selon vos désirs. Si vous sélectionnez la configuration 'personnalisée', vous accéderez automatiquement aux différents dialogues après avoir cliqué sur 'Suivant'. Vous trouverez ici les valeurs définies lors de l'installation.

'Configuration du mot de passe' Si vous souhaitez que le système vérifie les nouveaux mots de passe avant de les accepter, activez les deux cases à cocher 'Vérification des nouveaux mots de passe' et 'Vérifier la plausibilité

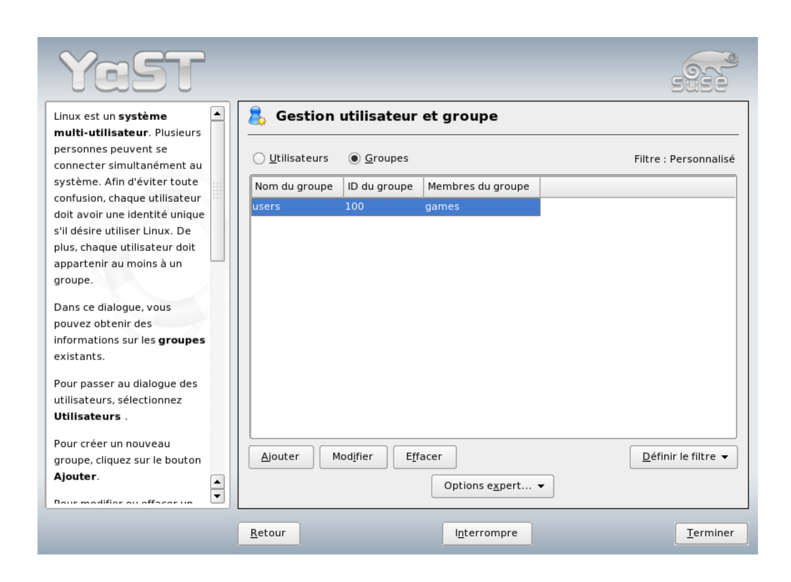


FIG. 2.8: *Gestion des groupes*

des mots de passe'. Spécifiez la longueur minimale et maximale des mots de passe pour les nouveaux utilisateurs ainsi que la période de validité du mot de passe, sa date d'expiration et préciser combien de jours avant l'expiration l'utilisateur devra en être averti.

'Paramètres d'amorçage' Spécifiez ici de quelle manière la combinaison de touches Ctrl-Alt-Delete doit être interprétée en sélectionnant l'action désirée. Sur la console texte, cette combinaison de touches déclenche habituellement un redémarrage du système. Il est en principe préférable de ne rien changer ici à moins que votre machine ou votre serveur ne soit accessible à d'autres utilisateurs et que vous ayez lieu de craindre que quelqu'un puisse effectuer cette action sans autorisation. Si vous sélectionnez 'Stop', cette combinaison de touches déclenchera un arrêt du système et si vous choisissez 'Ignorer', elle ne provoquera plus rien.

Spécifiez également le 'Comportement d'arrêt de KDM' en attribuant des permissions pour arrêter le système à partir de KDM (KDE Display Manager), le login graphique de KDE. Donnez la permission à 'Seulement root' (l'administrateur du système), 'Tous les utilisateurs', 'Personne' ou aux 'Utilisateurs locaux'. Si vous sélectionnez 'Personne', le système ne pourra être arrêté qu'à partir de la console texte.

'Paramètres de login' Après une tentative de connexion qui s'est soldée par un échec, on doit normalement attendre quelques secondes avant de pouvoir recommencer. Cette règle a pour but de rendre la vie dure aux casseurs de mots de passe. Vous avez en outre la possibilité d'activer les options 'Enregistrer les tentatives de login échouées' et 'Enregistrer les tentatives de login réussies'. Si vous soupçonnez que quelqu'un cherche à deviner votre mot de passe, vous pouvez contrôler les entrées dans les fichiers de traces du système sous `/var/log`. Avec l'option 'Permettre le login graphique à distance', les autres utilisateurs pourront accéder à l'écran de login graphique à travers le réseau. Cependant, cette possibilité d'accès représente un risque potentiel pour votre sécurité et est donc désactivée par défaut.

'Ajouter des paramètres utilisateur' Chaque utilisateur possède un identificateur numérique et un identificateur alphanumérique. L'association entre ces deux identificateurs se fait dans le fichier `/etc/passwd` et ne devrait présenter aucune ambiguïté. Les données affichées ici vous permettent de voir les zones de valeurs utilisées pour la partie numérique d'un identificateur lorsqu'un nouveau compte utilisateur est créé. Le minimum fixé à 500 pour un utilisateur est une valeur raisonnable et devrait être considéré comme la limite inférieure à ne pas dépasser ; les numéros générés automatiquement commencent à 1000. Procédez de la même façon pour la configuration des identificateurs de groupes.

'Paramètres divers' Vous avez trois possibilités de définir la 'Configuration des droits d'accès aux fichiers'. Vous avez le choix entre 'Easy', 'Secure' et 'Paranoid'. Pour la plupart des utilisateurs, la première option est suffisante. Le texte d'aide de YaST vous informe sur ces trois niveaux de sécurité. L'option 'Paranoid' est extrêmement restrictive et devrait être utilisée par un administrateur système comme base pour une configuration personnalisée. Si vous choisissez 'Paranoid', vous devrez vous attendre à des perturbations ou dysfonctionnements lors de l'exécution de certains programmes car vous n'avez plus les droits nécessaires pour accéder à différents fichiers.

Dans ce dialogue, vous pouvez en outre déterminer l'utilisateur qui devra lancer le programme `updatedb`. Ce programme qui est exécuté automatiquement tous les jours ou après chaque amorçage génère une base de données (locatedb) dans laquelle est enregistré l'emplacement de chaque fichier. Si vous sélectionnez 'Personne', il ne sera possible de trouver dans la base de données que les chemins d'accès que n'importe quel utilisateur (sans privilège) pourrait voir. Si vous sélectionnez `root`, tous les fichiers locaux seront indexés puisque l'utilisateur `root` est autorisé, en tant que super-utilisateur, à lister tous les répertoires. Enfin, assurez-vous que l'option 'Répertoire courant dans le chemin de l'utilisateur root' est désactivée (par défaut).

En cliquant sur 'Terminer', vous achèverez la configuration des paramètres de sécurité de votre système.



FIG. 2.9: *Paramètres de sécurité*

2.6.4 Pare-feu

Ce module vous permet de mettre en place et de configurer de façon très simple le pare-feu SuSEfirewall2 pour protéger votre système des intrus venant d'Internet. Vous trouverez des informations détaillées relatives à SuSEfirewall2 dans la section 34.1 page 630.

Astuce

Démarrage automatique du pare-feu

Sur chaque interface réseau configurée, YaST démarre automatiquement un pare-feu avec les paramètres appropriés. Vous n'avez donc besoin de ce module que si vous souhaitez procéder à une configuration plus avancée du pare-feu ou si vous souhaitez le désactiver complètement.

Astuce

2.7 Système

2.7.1 Copie de sauvegarde des zones du système

Avec le nouveau module de sauvegarde, vous avez la possibilité d'effectuer une sauvegarde de votre système avec YaST. La sauvegarde effectuée avec ce module ne contient pas le système complet. Elle enregistre uniquement des informations sur les paquetages modifiés, les zones système critiques et les fichiers de configuration.

Lors de la configuration, vous pouvez décider quels fichiers devront être sauvegardés. Par défaut, les informations concernant les paquetages qui ont été modifiés depuis la dernière installation seront enregistrées. Vous pouvez, en outre, stocker dans votre répertoire `/etc` ou dans votre répertoire `home`, des fichiers qui n'appartiennent à aucun paquetage, par exemple de nombreux fichiers de configuration. Vous pouvez également ajouter les zones système critiques du disque dur telles que les tables des partitions ou le secteur d'amorçage (MBR) qui pourront être utilisées dans le cas d'une éventuelle restauration.

2.7.2 Restauration du système

Avec le module de restauration que vous pouvez voir dans la figure 2.10 page suivante), vous pouvez restaurer votre système à partir d'une copie de sécurité. Suivez les instructions dans YaST. En cliquant sur 'Suivant', vous ouvrez les différents dialogues. Entrez tout d'abord à quel endroit se trouvent les archives (support amovible, disque local ou encore système de fichiers du réseau). Vous obtenez ensuite les descriptions et contenus correspondants à la copie et vous pourrez sélectionner ce que vous voulez récupérer.

En outre, il existe un dialogue dans lequel vous pouvez choisir de désinstaller les paquetages qui ont été ajoutés depuis la dernière copie de sauvegarde et un dialogue dans lequel vous pouvez procéder à la réinstallation des paquetages qui ont été supprimés depuis la dernière copie de sauvegarde. À l'aide de ces deux étapes supplémentaires, vous pouvez restaurer votre système exactement dans le même état que lors de la dernière sauvegarde.

Avertissement

Restaurer le système

Étant donné que ce module permet normalement d'installer, de remplacer ou de désinstaller de nombreux paquetages et fichiers, nous vous conseillons de ne l'utiliser que si vous avez l'habitude de manipuler les copies de sauvegarde. Dans le cas contraire, vous pourriez perdre des données.

Avertissement

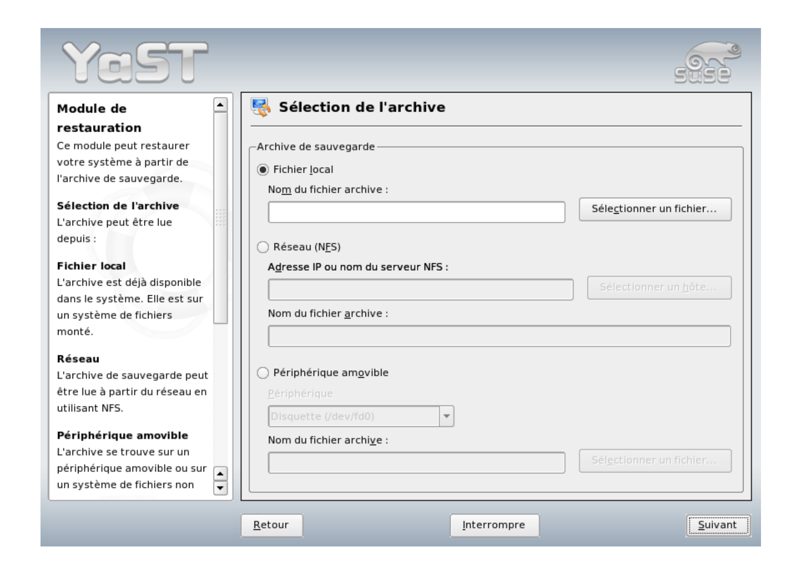


FIG. 2.10: *YaST~: Fenêtre de démarrage du module de restauration*

2.7.3 Création d'une disquette d'amorçage et de secours

Avec ce module de YaST, vous pouvez créer des disquettes d'amorçage et de secours. Ces disquettes vous seront utiles au cas où la configuration de démarrage de votre système se détériorerait. La disquette de secours est tout spécialement nécessaire si le système de fichiers de la partition root est abimé.

Vous disposez des options suivantes :

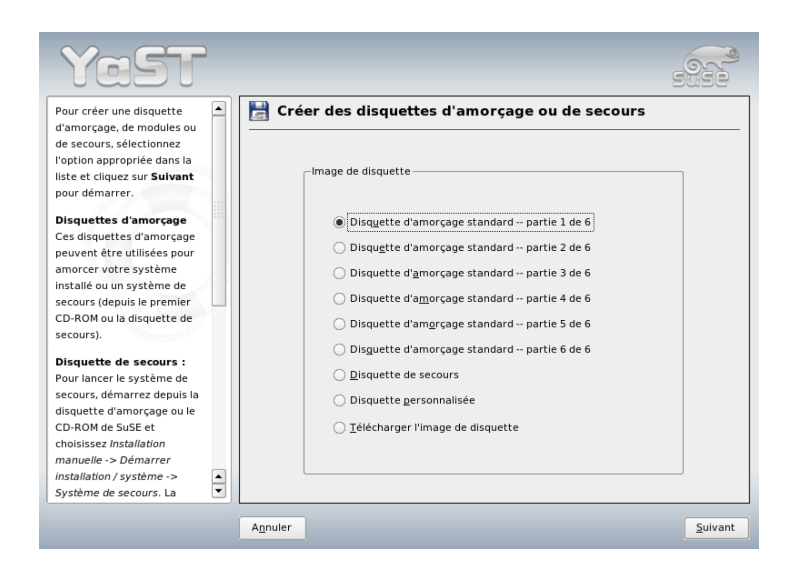


FIG. 2.11: *Création de disquettes d'amorçage et de secours*

'Disquette d'amorçage standard' Avec cette option, vous pouvez créer les disquettes de démarrage standard pour amorcer un système déjà installé. Selon l'architecture, le nombre de disquettes d'amorçage peut varier mais vous devriez créer toutes les disquettes présentées dans le dialogue parce qu'elles sont toutes nécessaires à l'amorçage. Ces disquettes sont également nécessaires à l'amorçage du système de sauvegarde.

'Disquette de secours' Cette disquette contient un environnement spécial qui vous permet d'effectuer des travaux de réparation ou de maintenance dans un système déjà installé, par exemple, vérifier les systèmes de fichiers et actualiser le gestionnaire de démarrage. Pour démarrer le système de secours, amorcez tout d'abord avec les disquettes d'amorçage standard puis sélectionnez 'Installation manuelle', 'Démarrer installation ou système' et 'Système de secours'. L'insertion de la disquette de secours vous sera alors demandée.

'Disquette personnalisée' Cette option vous permet de copier une image disquette quelconque du disque dur vers la disquette. Ce fichier image doit déjà exister sur le disque dur.

'Télécharger une image disquette' Cette option vous permet de télécharger une image disquette depuis Internet après avoir saisi l'URL et les données d'authentification correspondants.

Pour créer les disquettes citées ci-dessus, sélectionnez l'option appropriée et cliquez sur 'Suivant'. Insérez une disquette comme cela vous est demandé. Cliquez encore une fois sur 'Suivant', le contenu correspondant à l'option sera alors écrit sur la disquette.

2.7.4 LVM

Le gestionnaire de volumes logiques (Logical Volume Manager, LVM) est un outil permettant le partitionnement individuel du disque dur au moyen de disques logiques. Vous trouverez plus d'informations à ce sujet dans la section 3.7 page 104.

2.7.5 Partitionnement

Dans le dialogue pour experts représenté dans la figure 2.12 page suivante, modifiez manuellement le partitionnement d'un ou plusieurs disques durs. Vous avez la possibilité d'ajouter, de supprimer ou de modifier des partitions. Vous pouvez également accéder au RAID logiciel et à la configuration LVM depuis ce module YaST.

Avertissement

Bien qu'il soit possible de modifier les partitions dans le système installé, cela ne devrait être fait que par des experts. Dans le cas contraire, le risque de perdre des données est très haut. Si vous procédez à un nouveau partitionnement du disque dur utilisé, réamorcez le système immédiatement après. Il est plus sûr d'utiliser le système de secours plutôt que de procéder au repartitionnement du système en fonctionnement.

Avertissement

Le dialogue affiche une liste de toutes les partitions existantes ou proposées sur tous les disques durs. Les disques dans leur intégralité sont représentés comme des périphériques sans numéros, comme `/dev/hda` ou `/dev/sda` alors que les partitions sont représentées en tant que parties de ces périphériques et sont numérotées, comme `/dev/hda1` ou `/dev/sda1`. La taille, le type, le système de fichiers et le point de montage de chaque disque et partition sont affichés. Le point

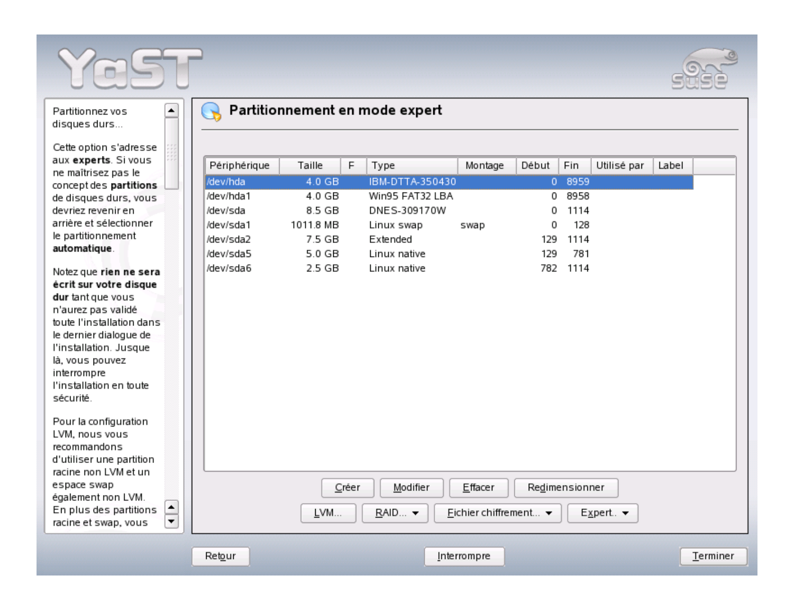


FIG. 2.12: *Le partitionneur pour expert de YaST*

de montage indique l'emplacement de l'arborescence Linux où la partition a été rattachée.

Si vous passez dans le dialogue pour experts lors de l'installation, l'espace libre sur le disque dur est également affiché et sélectionné automatiquement. Si vous voulez attribuer plus d'espace disque à SUSE LINUX, libérez l'espace nécessaire en allant de bas en haut (c'est à dire de la dernière d'un disque dur à la première). Ainsi, si vous avez trois partitions par exemple, il n'est pas possible de choisir exclusivement la deuxième des trois partitions pour SUSE LINUX et de laisser la première et la troisième pour un autre système d'exploitation.

Créer une partition

Sélectionnez 'Créer'. Si vous avez plusieurs disques durs, une fenêtre de dialogue dans laquelle vous pouvez marquer le disque dur sur lequel vous voulez créer la nouvelle partition. Ensuite, spécifiez le type de la partition (primaire ou étendue). Vous pouvez créer jusqu'à quatre partitions primaires ou trois partitions primaires et une partition étendue dans laquelle il vous est possible de créer plusieurs partitions logiques (à ce sujet, consultez la section Types de partition page 12).

Sélectionnez maintenant le système de fichiers et, si nécessaire, un point de montage. YaST vous propose un point de montage pour chaque partition que vous créez. Vous trouverez des détails relatifs aux paramètres dans la section suivante. Cliquez sur 'OK' pour que les modifications deviennent effectives. La nouvelle partition est alors ajoutée à la table des partitions. Si vous cliquez sur 'Suivant', les valeurs actuelles seront appliquées. Lors d'une installation, la fenêtre de dialogue apparaît à nouveau.

Paramètres de partitionnement

Lorsque vous créez une nouvelle partition dans l'arborescence des fichiers ou que vous modifiez une partition existante, vous pouvez définir différents paramètres. Dans le cas de nouvelles partitions, YaST se charge de fixer ces paramètres et normalement, vous n'aurez pas à faire de changement. Cependant, si vous souhaitez réaliser une configuration manuelle, procédez comme suit :

1. Selection de la partition
2. 'Modification' de la partition et réglage des paramètres :

Identificateur du système de fichiers
Même si vous ne voulez pas formater la partition ici, vous devez indiquer au moins l'identificateur du système de fichiers pour être certain que la partition soit enregistrée correctement. Les valeurs possibles sont, par exemple, 'Linux', 'Linux swap', 'Linux LVM' et 'Linux RAID'. Vous trouverez plus de détails au sujet de LVM et RAID dans la section 3.7 page 104 et la section 3.8 page 111.

Système de fichiers Si vous souhaitez formater la partition dès l'installation, vous pouvez indiquer ici l'un des systèmes de fichiers suivants pour la partition : 'Swap', 'Ext2', 'Ext3', 'ReiserFS' et 'JFS'. Vous trouverez des détails relatifs aux différents systèmes de fichiers dans le chapitre 20 page 389.

Swap est un format spécial qui permet d'utiliser la partition en tant que mémoire virtuelle. ReiserFS est le système de fichiers par défaut pour les partitions Linux. ReiserFS, tout comme JFS et Ext3, est un système de fichiers avec journalisation (Journaling Filesystem). Un tel système de fichiers peut rétablir votre système très rapidement après un plantage éventuel, car la journalisation se fait durant le fonctionnement du système. En outre, ReiserFS est très efficace dans la gestion de grandes quantités de petits fichiers. Ext2 n'est pas un système de

fichiers avec journalisation, mais il est très stable et particulièrement approprié pour les petites partitions, car il ne nécessite que peu d'espace disque pour sa propre gestion.

Options du système de fichiers Ici, vous pouvez configurer divers paramètres du système de fichiers sélectionné. Selon le système de fichiers utilisé, différentes options s'offrent aux experts.

Chiffrement d'un système de fichiers
Si vous activez le chiffrement, toutes les données de votre disque dur seront chiffrées. Ceci augmente le niveau de sécurité des données sensibles, mais le système s'en trouve ralenti car ce processus de chiffrement requiert du temps. Vous trouverez plus d'informations relatives au chiffrement des systèmes de fichiers dans la section 34.3 page 646.

Options fstab Ici, vous pouvez spécifier différents paramètres pour le fichier d'administration des systèmes de fichiers (`/etc/fstab`).

Point de montage Ici est indiqué le répertoire de l'arborescence du système de fichiers dans lequel la partition doit être montée. Choisissez parmi plusieurs suggestions que vous fait YaST ou entrez un autre nom.

3. Cliquez sur 'Suivant' pour activer la partition.

Lorsque vous procédez manuellement à un partitionnement, vous devez créer une partition swap d'au moins 256 Mo. La partition swap sert à libérer temporairement le disque dur des données non nécessaires en cet instant afin de toujours conserver la mémoire vive disponible pour les données les plus importantes et les plus utilisées.

Options pour expert

'Expert' ouvre un menu contenant les commandes suivantes :

Relire la table de partitions Relit le partitionnement depuis le disque. Vous avez besoin de cette option après le partitionnement manuel dans la console de texte, par exemple.

Supprimer la table de partitions et le label disque
Écrase complètement l'ancienne table de partitions. Par exemple, ceci peut vous être utile si vous avez des problèmes avec des labels de disque non conventionnels. Si vous utilisez cette méthode, vous perdrez toutes les données sur le disque dur.

Informations complémentaires sur le partitionnement

Si YaST effectue automatiquement le partitionnement et constate que d'autres partitions sont présentes dans votre système, celles-ci seront également inscrites dans le fichier /etc/fstab afin qu'il soit possible d'accéder simplement à ces données. Dans ce fichier, toutes les partitions présentes sur votre système sont répertoriées avec les propriétés qui leur correspondent, telles que système de fichiers, point de montage et droits d'utilisateur.

Example 2.1: */etc/fstab : données des partitions*

```
/dev/sda1    /data1    auto      noauto,user 0 0
/dev/sda5    /data2    auto      noauto,user 0 0
/dev/sda6    /data3    auto      noauto,user 0 0
```

Les partitions, qu'il s'agisse de partitions Linux ou de partitions FAT, sont enregistrées avec les options noauto et user. Chaque utilisateur peut ainsi monter ou démonter ces partitions en cas de besoin. Pour des raisons de sécurité, YaST n'entre pas automatiquement l'option exec ici. Cette option est néanmoins nécessaire pour exécuter d'ici des programmes. Si vous désirez cependant exécuter des programmes ou des scripts, saisissez vous-même cette option. Cette option est nécessaire lorsque vous voyez apparaître des messages tels que bad interpreter ou permission denied.

Partitionnement et LVM

Depuis le partitionneur pour experts, accédez à la configuration LVM avec 'LVM' (voir la section 3.7 page 104). Cependant, si une configuration LVM qui fonctionne existe déjà sur votre système, elle est automatiquement activée dès que vous entrez dans la configuration LVM pour la première fois lors d'une session. Dans ce cas, tout disque contenant une partition qui appartient à un groupe volume actif ne peut pas être repartitionnée parce que le noyau Linux ne peut pas relire la table de partitions modifiée d'un disque dur lorsqu'une partition de ce disque est en cours d'utilisation. Néanmoins, si vous avez déjà une configuration LVM qui fonctionne sur votre système, le repartitionnement physique ne devrait pas être nécessaire. Changez plutôt la configuration des volumes logiques.

Au début des volumes physiques (VP), les informations relatives au volume sont écrites sur la partition. De cette façon, un VP "sait" à quel groupe il appartient. Pour réutiliser une telle partiton à d'autres fins non LVM, il est conseillé d'effacer le début de ce volume. Par exemple, dans le système VG et /dev/sda2 VP, ceci peut être fait à l'aide de la commande dd if=/dev/zero of=/dev/sda2 bs=512 count=1.

Avertissement

Système de fichiers pour l'amorçage

Le système de fichiers utilisé pour l'amorçage (le système de fichiers root ou `/boot`) ne doit pas être enregistré sur un volume logique LVM. Enregistrez-le plutôt sur une partition physique normale.

Avertissement

2.7.6 Gestionnaire de profils (SCPM)

Le module pour le gestionnaire de profils (SCPM, system configuration profile management) vous offre la possibilité de créer des configurations du système individuelles complètes, de les gérer et de passer de l'une à l'autre à volonté. Normalement, une telle propriété peut être très utile, surtout dans le cas des ordinateurs portables qui sont utilisés dans des endroits différents (dans des réseaux différents) par des personnes différentes. Cependant, cela peut également être utile dans le cas d'ordinateurs stationnaires afin de pouvoir utiliser différents matériels ou différentes configurations de test. Si vous souhaitez obtenir des informations complémentaires au sujet du gestionnaire de profils SCPM et de son utilisation, veuillez vous consulter le chapitre 15 page 309.

2.7.7 Éditeur de niveaux d'exécution

Vous pouvez utiliser SUSE LINUX dans différents niveaux d'exécution (runlevel). Par défaut, le système est démarré dans le niveau d'exécution 5. Ceci signifie que la fonctionnalité multi-utilisateurs, l'accès au réseau et l'interface graphique (système X Window) sont activés. Les autres niveaux d'exécution vous proposent la fonctionnalité multi-utilisateurs avec accès au réseau sans X (niveau d'exécution 3), fonctionnalité multi-utilisateurs sans accès au réseau (niveau d'exécution 2), système mono-utilisateur (niveau d'exécution 1 et S), arrêt du système (niveau d'exécution 0) et réamorçage du système (niveau d'exécution 6).

Les différents niveaux d'exécution sont surtout utiles lorsque, dans un niveau d'exécution supérieur, un problème arrive dans le service correspondant (X ou réseau). Le système peut alors être démarré dans un niveau d'exécution inférieur afin de réparer le service en cause. En outre, beaucoup de serveurs fonctionnent sans interface graphique et ces ordinateurs doivent donc être amorcés dans le niveau d'exécution 3, par exemple.

Normalement, vous n'aurez besoin que du niveau d'exécution par défaut (5). Cependant, si l'interface graphique venait à se planter, vous pouvez redémarrer votre système X Window en passant dans une console texte à l'aide de la combinaison de touches Ctrl-Alt-F1, vous y connecter en tant qu'administrateur root puis passer dans le niveau d'exécution 3 à l'aide de la commande `init 3`. De cette façon, votre système X Window sera arrêté. Vous pouvez le redémarrer en saisissant simplement `init 5`.

Vous trouverez plus d'informations au sujet des niveaux d'exécution sous SUSE LINUX et une description de l'éditeur de niveaux d'exécution de YaST dans le chapitre 7 page 165.

2.7.8 Éditeur sysconfig

Dans le répertoire `/etc/sysconfig` se trouvent les fichiers qui contiennent les paramètres les plus importants pour SUSE LINUX. L'éditeur sysconfig présente toutes les possibilités de configuration de façon claire. Les valeurs peuvent être modifiées et enregistrées dans les différents fichiers de configuration. Cependant, la modification manuelle de ces valeurs n'est généralement pas nécessaire, étant donné que lors de l'installation d'un paquetage ou lors de la configuration d'un service, les fichiers sont actualisés automatiquement. Vous trouverez plus d'informations relatives à `/etc/sysconfig` à l'éditeur sysconfig de YaST dans le chapitre 7 page 165.

2.7.9 Sélection de la zone horaire

La zone horaire est déjà déterminée au cours de l'installation mais vous avez ici la possibilité de procéder encore à une modification. Dans la liste des pays, cliquez simplement sur le nom du vôtre et sélectionnez 'Heure locale' ou 'UTC' (Universal Time Coordinated, le temps universel coordonné qui a remplacé l'heure du méridien de Greenwich). Dans un système Linux, on utilise habituellement 'UTC'. Les machines sur lesquelles sont installés d'autres systèmes d'exploitation, par exemple Microsoft Windows, utilisent généralement l'heure locale.

2.7.10 Sélection de la langue

Procédez ici à la sélection de la langue pour votre système Linux. La configuration de la langue effectuée avec YaST s'étend à tout le système. Elle est donc valable pour YaST et le bureau.

2.8 Divers

2.8.1 Adresser une requête d'Assistance Technique à l'Installation

L'achat d'une distribution SUSE LINUX vous donne droit à l'assistance gratuite à l'installation. Vous trouverez des informations relatives à l'étendue du service, l'adresse et les numéros de téléphone sur notre page web `http://www.novell.com/linux/suse/`.

YaST vous donne la possibilité d'adresser directement une requête par courrier électronique au service d'Assistance Technique à l'Installation de SUSE. Vous pourrez bénéficier de ce service après enregistrement. Fournissez au début de votre requête les informations nécessaires—vous trouverez votre code d'enregistrement au dos de la pochette des CD. Sélectionnez dans la fenêtre suivante la catégorie de votre problème et décrivez-le (voir la figure 2.13 page suivante). Pour la rédaction de votre requête, lisez le texte d'aide de YaST qui vous informe de la meilleure manière de décrire votre problème afin que l'équipe d'assistance puisse vous venir en aide au plus vite.

Astuce

Si vous avez besoin d'une assistance plus avancée, par exemple pour des problèmes particuliers, vous trouverez des informations plus détaillées sous `http://support.novell.com/linux/`.

Astuce

2.8.2 Fichier de démarrage

Le journal de démarrage `/var/log/boot.msg` est le fichier qui contient les messages qui apparaissent à l'écran lors du démarrage de la machine. Avec ce module de YaST, vous pouvez l'afficher et vérifier, par exemple, si tous les services et fonctions ont été démarrés comme vous l'aviez prévu.

2.8.3 Fichier de traces du système

Le fichier de traces du système enregistre ce qui se passe sur votre machine et se trouve sous `/var/log/messsages`. Vous voyez apparaître ici les messages du noyau classés par date et heure.

FIG. 2.13: *Adresser une requête d'Assistance Technique à l'Installation*

2.8.4 Charger le CD de pilotes du fabricant

Avec ce module, vous pouvez installer automatiquement des pilotes de périphériques à partir d'un CD contenant des pilotes pour SUSE LINUX. Si vous procédez à une nouvelle installation de votre système SUSE LINUX, ce module de YaST vous donne la possibilité, après installation, de charger les pilotes indispensables à partir du CD du fabricant.

2.9 YaST en mode texte (ncurses)

Cette section s'adresse principalement aux administrateurs de système et aux experts dont les machines n'exécutent pas de serveur X et qui doivent utiliser l'utilitaire d'installation en mode texte. Vous trouverez dans cette section des informations de base sur l'exécution et l'utilisation de YaST en mode texte (ncurses).

Lorsque vous lancez YaST en mode texte, le centre de contrôle YaST apparaît d'abord (voir figure 2.14 page suivante). On distingue ici trois rubriques : sur le

volet gauche, dans un cadre blanc épais, on peut voir les catégories auxquelles sont rattachés les différents modules. La catégorie courante est mise en surbrillance. Le volet droit, pourvu d'un fin cadre blanc, présente les différents modules appartenant à la catégorie active. Le volet inférieur, enfin, comporte les boutons 'Aide' et 'Quitter'.

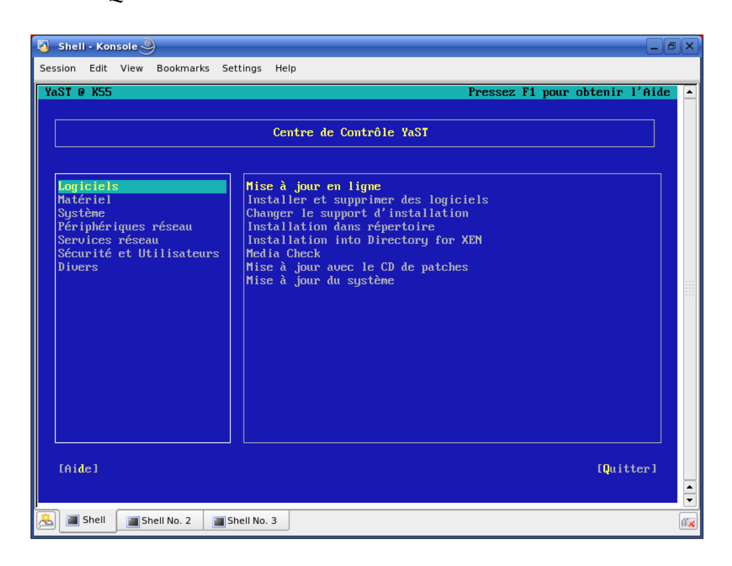


FIG. 2.14: *Écran principal de YaST en mode texte*

Lors du démarrage du centre de contrôle de YaST, la catégorie 'Logiciels' est sélectionnée automatiquement. Pour changer de catégorie, appuyez sur les touches ↓ et ↑. Pour lancer un module depuis la catégorie sélectionnée, utilisez la touche →. Le module sélectionné apparaît alors avec dans un cadre épais. Sélectionnez le module de votre choix à l'aide des touches ↓ et ↑. Tout en maintenant la touche de direction enfoncée, faites défiler les différents modules disponibles . Dès que vous avez sélectionné un module, le titre correspondant apparaît en surbrillance. Parallèlement, une description succincte du module s'affiche sur le volet inférieur.

Appuyez sur la touche Enter pour lancer le module choisi. Le module comporte différents boutons ou zones de sélection avec une lettre de couleur différente (jaune, dans la configuration par défaut). La combinaison de touches Alt–lettre_jaune vous permet de sélectionner directement le bouton en question en

vous épargnant d'utiliser laborieusement la touche de navigation Tab. Pour quitter le centre de contrôle de YaST, vous pouvez soit utiliser le bouton 'Quitter', soit sélectionner le sous-menu 'Quitter' de la liste des catégories, puis appuyer sur la touche Enter.

2.9.1 Navigation dans les modules

Dans la description suivante de l'interface des modules de YaST, nous faisons l'hypothèse que les touches de fonctions et les combinaisons utilisant la touche Alt fonctionnent correctement, et n'ont pas été modifiées pour l'ensemble du système. Pour plus d'informations sur les exceptions possibles, lisez section 2.9.2 page suivante.

Navigation entre les boutons et listes de sélection
Les touches Tab et Alt-Tab ou Maj-Tab vous permettent de naviguer parmi les boutons et les cadres des listes de sélection.

Navigation dans les listes de sélection
Dans un cadre activé dans lequel se trouve une liste de sélection, c'est à l'aide des flèches (↑ et ↓) que vous pouvez naviguer entre les différents éléments. Si certaines lignes ont une longueur supérieure à celle du cadre et que leur texte dépasse de ce cadre, vous pouvez faire défiler le contenu du cadre horizontalement vers la droite au moyen de Maj-→ ou vers la gauche avec Maj-←. Une solution alternative consiste à utiliser Ctrl-E ou Ctrl-A. Cette combinaison fonctionne également là où → et ← provoquent un saut du cadre actif vers le cadre suivant ou de la liste de sélection active vers la liste suivante, comme c'est le cas dans le centre de contrôle.

Boutons, boutons radio et cases à cocher
Pour actionner des boutons représentés par des crochets vides (cases à cocher) ou par des parenthèses vides (boutons radio), appuyez sur la touche Espace ou Enter. Il est également possible d'activer directement les boutons radio et cases à coche au moyen de Alt-lettre_jaune. Dans ce cas, vous n'avez pas besoin de confirmer avec Enter. Pour la navigation par tabulation, il est nécessaire d'appuyer encore une fois sur la touche Entrée pour exécuter l'action sélectionnée ou activer le point de menu correspondant.

Les touches de fonction Les touches de fonction (F1 à F12) permettent l'accès rapide à divers boutons. L'affectation d'une touche de fonction donnée à une fonction dépend du module de YaST dans lequel vous vous trouvez. En

effet, les différents modules comportent chacun leurs propres boutons (tels que Détails, Ajouter, Supprimer, etc.). Utilisez la touche de fonction F10 pour 'OK', 'Suivant' et 'Terminer'. L'aide de YaST, à laquelle vous accédez en appuyant sur la touche F1, vous fournira la table de correspondance entre les fonctions et les touches de fonction associées.

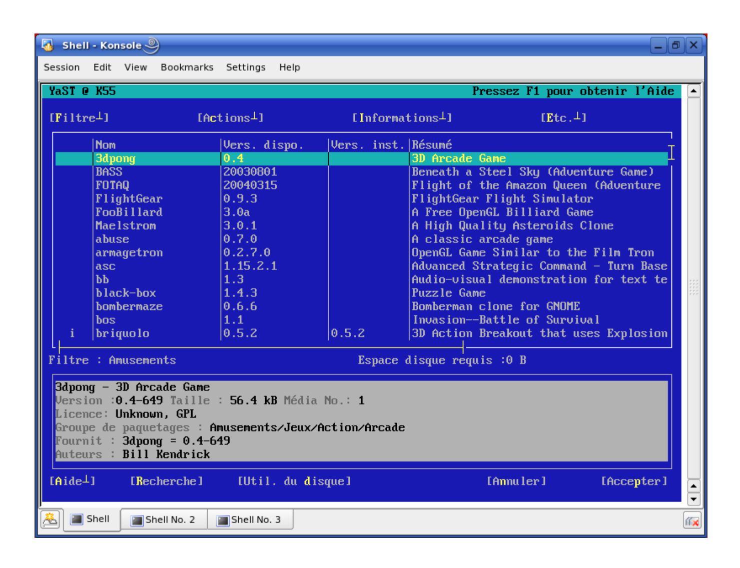


FIG. 2.15: *Le module d'installation de logiciels*

2.9.2 Restrictions sur les combinaisons de touches

Si votre gestionnaire de fenêtres utilise des combinaisons de touches globales (pour l'ensemble de votre système) utilisant Alt, il est possible que, dans YaST, les combinaisons de touches utilisant Alt ne fonctionnement pas. De même, les touches Alt ou Maj peuvent également avoir été affectées par les paramètres du terminal utilisé.

Substitution de la touche Alt par la touche Esc

Les raccourcis utilisant la touche Alt peuvent être exécutés avec Esc au lieu de Alt. Ainsi, Esc–H remplace la combinaison de touches Alt–H.

Navigation en avant et en arrière au moyen des combinaisons Ctrl–F et Ctrl–B
Dans le cas où les combinaisons de touches Alt et Maj sont réservées par le gestionnaire de fenêtres ou par le terminal, vous pouvez utiliser à la place les combinaisons Ctrl–F (suivant, en anglais forward) et Ctrl–B (précédent, en anglais backward).

Restriction des touches de fonction : Les touches de fonction sont également utilisées. Il est possible que certaines touches de fonctions soient réservées par le terminal et qu'elles ne soient donc pas disponibles pour YaST. Toutefois, une pure console texte devrait continuer à avoir pleinement accès aux combinaisons de touches Alt et aux touches de fonction.

2.9.3 Exécution des différents modules

Vous pouvez également gagner du temps en démarrant directement chacun des modules de YaST. Pour démarrer un module, saisissez `yast <nommodule>`. Par exemple, le module réseau est lancé à l'aide de la commande `yast lan`. Vous pouvez obtenir la liste de tous les noms de modules disponibles sur votre système en exécutant la commande `yast -l` ou `yast --list`.

2.9.4 Le module YOU

À la ligne de commande, vous pouvez en tant qu'utilisateur `root`, démarrer le module de mise à jour en ligne de YaST ("YaST Online Update" ou YOU) comme tout autre module de YaST :

```
yast online_update .url <url>
```

`yast online_update` démarre le module correspondant. Au moyen de l'option `url`, vous indiquez à YOU un serveur (local ou sur Internet) à partir duquel récupérer tous les correctifs et les informations. Si cette information n'est pas fournie au premier appel à YOU, vous pouvez renseigner le serveur ou le répertoire dans le dialogue de YaST. Avec le bouton 'Configurer mise à jour automatisée', vous pouvez configurer une tâche cron pour procéder à l'automatisation de la mise à jour.

2.10 Online Update (Mise à jour en ligne) en ligne de commande

Vous pouvez mettre à jour votre système de façon totalement automatisée, par exemple au moyen de scripts, avec l'outil en ligne de commande online_update. Vous pouvez souhaitez, par exemple, que votre système recherche des correctifs sur un serveur donné, de façon régulière et à des moments précis, télécharge les correctifs et les informations correspondantes, mais n'effectue pas l'installation. Peut-être souhaitez-vous plutôt vérifier ultérieurement les correctifs et sélectionner ceux que vous souhaitez installer.

Pour utiliser cet outil, mettez en place une tâche cron qui exécute la commande suivante :

```
online_update -u <URL> -g <typemaj>
```

`-u`introduit l'URL de base de l'arborescence de répertoires à partir de laquelle les correctifs doivent être téléchargés. Les protocoles pris en charge sont les suivants : `http`, `ftp`, `smb`, `nfs`, `cd`, `dvd` et `dir`. L'option `-g` vous permet de télécharger les correctifs dans un répertoire local sans les installer. Vous disposez aussi d'une option permettant de contrôler le nombre de correctifs en fonction de trois types : `security` (mises à jour de sécurité), `recommended` (mises à jour conseillées) et `optional` (mises à jour optionnelles). Si vous ne précisez pas de type de mise à jour, online_update télécharge tous les nouveaux correctifs disponibles pour les types `security` et `recommended`.

Vous avez ensuite la possibilité d'installer immédiatement les paquetages téléchargés, sans explorer en détail et individuellement les correctifs. Les correctifs sont stockés par online_update dans le répertoire `/var/lib/YaST2/you/mnt`. Pour terminer l'installation des correctifs, utilisez la commande suivante :

```
online_update -u /var/lib/YaST2/you/mnt/ -i
```

Le paramètre `-u` spécifie l'URL local correspondant aux correctifs à installer. `-i` permet de démarrer la procédure d'installation.

Si vous souhaitez voir les correctifs téléchargés avant d'effectuer leur installation démarrez le dialogue YOU au moyen de :

```
yast online_update .url /var/lib/YaST2/you/mnt/
```

YOU démarre et utilise le répertoire local qui contient les correctifs précédemment téléchargés, plutôt qu'un répertoire distant sur Internet. Avec le gestionnaire de paquetages, sélectionnez ensuite les correctifs que vous souhaitez appliquer comme vous le faites pour des paquetages lors d'une installation.

À partir de la ligne de commande, il est possible de définir le comportement de la mise à jour en ligne YaST à l'aide de paramètres. La syntaxe à utiliser est la suivante : `online_update [paramètre ligne de commande]`. Les paramètres possibles et leur signification sont répertoriés dans la liste ci-après.

`-u URL` URL de base de l'arborescence de répertoires depuis laquelle les patches doivent être téléchargés.

`-g` Seulement télécharger les patches, ne pas les installer.

`-i` Installer les patches déjà chargés mais ne rien télécharger.

`-k` Vérifier si de nouveaux patches sont disponibles.

`-c` Afficher la configuration actuelle, sinon ne rien faire.

`-p produit` Produit pour lequel des patches doivent être récupérés.

`-v version` Version du produit pour laquelle des patches doivent être récupérés.

`-a architecture` Architecture de base du produit pour laquelle des patches doivent être récupérés.

`-d` ”Essai à vide“ (dry run). Télécharger les patches et simuler l'installation (le système demeure intact ; test uniquement).

`-n` Pas de vérification de la signature des fichiers téléchargés.

`-s` Afficher la liste des patches disponibles.

`-V` Mode prolixe (verbose). Affiche les messages du processus.

`-D` Mode débogage pour les experts et dans le but de la recherche d'erreur.

Plus d'informations relatives à online_update sont disponibles en saisissant `online_update -h`.

Procédures d'installation spéciales

SUSE LINUX peut être installé de nombreuses façons. Les variantes vont d'une installation rapide en mode graphique à une installation en mode texte qui permet de nombreux ajustements manuels. Vous trouverez ci-après les diverses-méthodes d'installation et des indications concernant l'utilisation de différentes sources d'installation dont le CD-ROM et NFS. Ce chapitre contient également des informations pour résoudre des problèmes rencontrés lors de l'installation et une section détaillée sur le partitionnement.

3.1 linuxrc

À chaque ordinateur, correspondent des routines BIOS spéciales qui sont exécutées lors de l'amorçage du sytèmes pour initialiser le matériel. Lors de la procédure d'amorçage en soi, ces routines chargent une image qui sera exécutée par l'ordinateur pour contrôler le processus d'amorçage qui suit. Normalement, cette image est un gestionnaire d'amorçage qui permet à l'utilisateur de sélectionner un sytème installé ou un système d'installation. Lors de l'installation de SUSE LINUX, une image d'amorçage est chargée ; celle-ci contient un noyau et un programme du nom de linuxrc.

linuxrc est un programme qui analyse et initialise le système pour le processus d'installation. Par défaut, il fonctionne sans interaction de la part de l'utilisateur et démarre YaST après avoir terminé. Si vous avez besoin de fournir des paramètres spéciaux à un module ou si la reconnaissance du matériel a échoué, vous pouvez avoir à exécuter linuxrc de façon interactive en démarrant l'installation manuelle.

Vous pouvez utiliser linuxrc non seulement lors de l'installation mais également comme un outil d'amorçage dans un système installé. Il est même possible de lancer un système de secours autonome s'exécutant en mémoire vive (sur le disque RAM). Pour plus de précisions, reportez-vous à la section 5.4 page 153.

Si le système utilise un disque initial RAM (initrd), un script appelé également linuxrc gère le chargement des modules lors de l'amorçage. Ce script est généré dynamiquement par le script `/sbin/mkinitrd`. Il est complètement différent du programme linuxrc utilisé pour l'installation et ne doit surtout pas être confondu avec celui-ci.

3.1.1 Passer des paramètres à linuxrc

Il est possible d'ajuster des paramètres à linuxrc qui changent le comportement du démarrage. linuxrc cherche un fichier Info, soit sur disquette, soit dans le fichier `initrd` du répertoire `/info`. C'est seulement à la suite de cette recherche que linuxrc lit les paramètres de l'invite du noyau. Les valeurs par défaut peuvent être modifiées dans le fichier `/linuxrc.config` qui est lu en premier lieu. Dans tous les cas, il vaut mieux enregistrer toute modification dans le fichier Info.

Astuce

Il est possible d'exécuter linuxrc en mode manuel. À cette fin, utilisez le paramètre "manual=1" à l'invite d'amorçage.

Astuce

Un fichier Info est constitué de mots-clés et des valeurs associées selon le modèle `key: value`. Ces paires de mots-clés/valeur peuvent aussi être transmises à l'invite d'amorçage du support d'installation sous cette forme. Le fichier `/usr/share/doc/packages/linuxrc/linuxrc.html` contient une liste de tous les mots-clés disponibles. Quelques uns des mots-clés les plus importants vous sont donnés ici, à titre d'exemple, avec des valeurs d'exemple :

Install: URL (nfs, ftp, hd, ...) Définir la source d'installation avec un `URL`. Les protocoles acceptés sont `cd`, `hd`, `nfs`, `smb`, `ftp`, `http` et `tftp`. La syntaxe correspond à la syntaxe habituelle telle qu'elle peut aussi être utilisé dans un navigateur, par exemple :

- `nfs://<serveur>/<répertoire>`
- `ftp://[utilisateur[:motdepasse]@]<serveur>/<répertoire>`

Netdevice: <eth0> Si vous disposez de plusieurs périphériques Ethernet, vous pouvez sélectionner l'interface que doit utiliser linuxrc à l'aide du paramètre `Netdevice:`.

HostIP: <10.10.0.2> Ceci définit l'adresse IP de l'ordinateur.

Gateway: <10.10.0.128> Lorsque le serveur d'installation n'est pas situé dans le même sous-réseau que l'ordinateur, il peut être atteint via la passerelle (gateway) par défaut.

Proxy: <10.10.0.1> Pour les connexions de type ftp et http, vous pouvez également utiliser un proxy. Celui-ci doit être défini à l'aide du paramètre `Proxy:`.

ProxyPort: <3128> Si le proxy n'utilise pas le port par défaut, cette option peut définir le port à utiliser.

Textmode: <0|1> Utilisez ce paramètre pour démarrer YaST en mode textuel.

VNC: <0|1> Pour pouvoir installer confortablement des ordinateurs qui ne possèdent pas de console graphique, il est possible d'utiliser VNC pour contrôler le processus d'installation. Le paramètre `VNC` active ce service sur le système d'installation. Voyez aussi le paramètre `VNCPassword`.

VNCPassword: <mot de passe> Définit le mot de passe pour définir les droits d'accès lors d'une installation VNC.

UseSSH: <0|1> Prépare un accès SSH à linuxrc. Ceci permet une installation avec YaST en mode textuel.

SSHPassword: <mot de passe> Prépare le mot de passe pour l'utilisateur `root` dans linuxrc.

Insmod: <paramètres module> Charge le module défini dans le noyau. Les paramètres nécessaires au chargement du module sont entrés séparés par des espaces.

AddSwap: <0|3|/dev/hda5> Avec une valeur à 0 pour ce mot-clé, la partition d'échange (swap) n'est pas activée. Si la valeur est positive, c'est la partition portant le numéro correspondant qui est activée. Il est également possible de donner directement le nom de la partition.

3.2 Installation via VNC

VNC (*Virtual Network Computing*) est une solution client-serveur qui permet d'accéder à un serveur X distant au moyen d'un client léger et facile à manipuler. Ce client est disponible pour différents systèmes d'exploitation tels que diverses versions de Microsoft Windows, Apples MacOS et Linux.

On utilise le client VNC, vncviewer, pour garantir l'affichage graphique et la manipulation de YaST pendant le processus d'installation. Avant le démarrage du système à installer, vous devez d'abord préparer l'ordinateur distant afin qu'il puisse accéder par le biais du réseau au système à installer.

3.2.1 Préparation de l'installation VNC

Pour effectuer une installation VNC, vous devez transmettre quelques paramètres au noyau, ceci devant avoir lieu avant l'amorçage du noyau. Pour ce faire, transmettez à l'invite de commande d'amorçage les options suivantes :

```
vnc=1 vncpassword=<xyz> install=<Quelle>
```

`vnc=1` signalise que le serveur VNC est démarré sur le système d'installation. En entrant `vncpassword`, vous transmettez le mot de passe qui sera utilisé plus tard. La source d'installation (`install`) peut soit être indiquée manuellement

(indication du protocole et de la page URL se référant au répertoire correspondant) soit contenir l'instruction `slp:/`. Dans le deuxième cas, la source d'installation est automatiquement recherchée par l'intermédiaire d'une demande SLP. Pour plus de détails sur SLP, consultez le chapitre 23 page 459.

3.2.2 Clients pour l'installation VNC

La connexion à l'ordinateur d'installation et au serveur VNC y étant exploité s'établit au moyen d'un client VNC. Sous SUSE LINUX, on utilise vncviewer qui fait partie du paquetage `xorg-x11-Xvnc`. Si vous souhaitez établir une connexion avec le système d'installation à partir d'un client Windows, vous devez installer dans le système Windows le programme tightvnc que vous trouverez sur le premier CD-ROM de SUSE LINUX dans le répertoire`/dosutils/tightvnc`.

Démarrez le client VNC de votre choix et entrez l'adresse IP du système d'installation ainsi que le mot de passe VNC dès que le programme vous invite à entrer ces indications.

Une solution alternative consiste à établir des connexions VNC également au moyen d'un navigateur internet compatible Java en entrant les informations suivantes dans le champ d'adresse internet du navigateur :

```
http://<IP-Adresse des Installationssystems>:5801/
```

Une fois la connexion établie, YaST est amorcé et vous pouvez commencer l'installation.

3.3 Installation en mode texte avec YaST

Au lieu de l'installer avec un assistant graphique, on peut installer SUSE LINUX à l'aide des menus en mode texte de YaST (mode console). Tous les modules de YaST sont eux aussi disponibles dans ce mode texte. On peut s'en servir en particulier lorsque l'on n'a pas besoin d'interface graphique, par exemple pour les systèmes serveurs, ou si la carte graphique n'est pas prise en charge par le système X Window. En utilisant ce mode d'installation, les malvoyants peuvent installer SUSE LINUX à l'aide de périphériques de sortie adéquats.

Vous devez tout d'abord configurer la séquence d'amorçage dans le BIOS de l'ordinateur afin qu'il s'amorce sur le lecteur de CD-ROM. Insérez le DVD ou le CD 1

dans le lecteur et redémarrez l'ordinateur. L'écran de démarrage apparaîtra au bout de quelques instants.

Avec les touches ↑ et ↓, choisissez 'Installation manuelle' dans un délai de 10 secondes, afin que le système installé *ne* démarre *pas* automatiquement. Saisissez les paramètres d'amorçage dans la ligne `boot options` si votre matériel l'exige. Toutefois, aucun paramètre particulier n'est en principe nécessaire. Si, comme langue d'installation, vous sélectionnez la langue de votre clavier, la disposition du clavier sera configurée correctement. Ceci simplifie la saisie des paramètres.

La touche F2 ('Mode graphique') permet de fixer la résolution d'écran pour l'installation. Choisissez 'Mode texte' si vous supposez que la carte graphique posera des problèmes pendant l'installation. Pour terminer, appuyez sur Entrée. Une barre de progression indiquant `Loading Linux kernel` (Amorçage du noyau Linux) apparaît, puis le noyau s'amorce et linuxrc démarre. Utilisez les menus de linuxrc pour effectuer l'installation.

D'autres problèmes d'amorçage se résolvent généralement à l'aide de paramètres de noyau. En cas de problèmes de DMA, on dispose de l'option de démarrage 'Installation—Safe Settings'. En cas de difficultés avec l'ACPI (Advanced Configuration and Power Interface) on peut jouer sur les paramètres de noyau suivants :

`acpi=off` Ce paramètre désactive le système ACPI complet. Il se justifie par exemple si votre ordinateur ne sait pas gérer l'ACPI du tout ou si vous soupçonnez fortement que l'ACPI est source de problèmes dans votre ordinateur.

`acpi=oldboot` Désactive presque complètement le système ACPI, seuls les éléments nécessaires à l'amorçage sont utilisés.

`acpi=force` Active ACPI même si votre ordinateur a un BIOS antérieur à 2000. Ce paramètre prend le pas sur `acpi=off`.

`pci=noacpi` Ce paramètre désactive le détournement d'IRQ PCI du nouveau système ACPI.

Recherchez également les articles de la base de données d'assistance sur `https://portal.suse.com` à l'aide du mot-clé *acpi*.

Choisissez 'Memory Test' dans le menu d'amorçage pour contrôler la mémoire si des difficultés "inexplicables" surviennent lors du chargement du noyau ou au cours de l'installation. Linux impose des exigences élevées en ce qui concerne le matériel. La mémoire et son temps de latence doivent être parfaitement ajustés ! Vous trouverez plus d'informations dans la base de données d'assistance à l'aide du mot-clé *memtest86*. Le mieux est d'effectuer le test de mémoire durant la nuit.

3.4 Démarrer SUSE LINUX

Après l'installation, il reste à déterminer comment vous souhaitez démarrer Linux au quotidien. L'aperçu qui suit présente les différentes possibilités d'amorçage de Linux. La meilleure méthode pour vous dépend surtout de l'utilisation que vous prévoyez.

Chargeur d'amorçage Linux La solution la plus propre techniquement et la plus universelle consiste à utiliser un gestionnaire d'amorçage Linux comme GRUB (Grand Unified Bootloader) ou LILO (Linux Loader), qui permet de choisir entre différents systèmes d'exploitation avant l'amorçage. Le chargeur d'amorçage peut être configuré dès l'installation ou ultérieurement à l'aide de YaST.

Disquette d'amorçage Vous pouvez démarrer Linux au moyen d'une *disquette d'amorçage*. Cette méthode ne fonctionne que si vous disposez d'un lecteur de disquettes. La disquette d'amorçage peut être générée avec YaST. À ce sujet, voyez la section 2.7.3 page 73

La disquette d'amorçage est aussi une solution provisoire judicieuse si vous ne maîtrisez pas encore les autres possibilités ou si vous souhaitez différer votre décision à propos du mécanisme d'amorçage définitif. De plus, si vous utilisez aussi un autre système d'exploitation, la disquette d'amorçage peut également être une bonne solution.

Avertissement

Certains BIOS vérifient la structure du secteur d'amorçage (MBR) et affichent faussement une alerte de virus après que l'on ait installé GRUB ou LILO. Pour résoudre ce problème, entrez dans le BIOS et cherchez les paramètres correspondants. Désactivez, par exemple, la 'protection contre les virus'. Vous pourrez réactiver cette option plus tard. Cependant, cette fonctionnalité est superflue si Linux est votre unique système d'exploitation.

Avertissement

Vous trouverez une étude détaillée des différentes méthodes d'amorçage dans le chapitre 8 page 183.

3.4.1 L'écran graphique SUSE

Depuis SUSE LINUX 7.2, l'écran graphique SUSE apparaît sur la première console lorsque l'option "vga=<valeur>" est utilisée en tant que paramètre noyau. Au moment de l'installation avec YaST, cette option est réglée automatiquement en fonction de la résolution choisie et de la carte graphique utilisée.

3.4.2 Désactiver l'écran SUSE

Vous disposez de trois possibilités pour désactiver l'écran SUSE :

Désactiver l'écran SUSE à la demande.
Saisissez la commande `echo 0 >/proc/splash` sur la ligne de commande pour désactiver l'écran graphique. Pour le réactiver, entrez `echo 1 >/proc/splash`.

Désactiver l'écran SUSE par défaut. Ajoutez à la configuration du chargeur d'amorçage le paramètre de noyau `splash=0`. Vous trouverez davantage d'informations à ce propos dans le chapitre 8 page 183. Toutefois, si vous préférez le mode texte qui était proposé par défaut sur les versions antérieures, saisissez `vga=normal`.

Désactiver définitivement l'écran SUSE.
Compilez un nouveau noyau et désactivez l'option 'Use splash screen instead of boot logo' dans le menu 'framebuffer support'.

Astuce

L'écran de démarrage est automatiquement désactivé lorsque vous avez désactivé le prise en charge du framebuffer dans le noyau. Si vous compilez votre propre noyau, SUSE ne peut pas garantir de services d'assistance pour le système.

Astuce

3.5 Trucs et astuces

Sur certains ordinateurs, il n'y a pas de lecteur de CD-ROM, mais un lecteur de disquettes amorçable. Pour installer sur un tel système, vous devez créer une disquette amorçable et l'utiliser pour amorcer le système.

Il vous faut des disquettes HD 3,5 pouces formatées pour créer une disquette amorçable à partir des images qui sont fournies. Le répertoire `boot` du CD 1 contient quelques images de disquettes. De telles images peuvent être copiée sur des disquettes grâce à un programme utilitaire approprié. Une disquette ainsi préparée s'appelle un disquette d'amorçage.

En outre, les images de disquettes renferment aussi le chargeur (loader) Syslinux et le programme linuxrc. Syslinux permet de choisir le noyau souhaité pendant le processus d'amorçage et au besoin de passer des paramètres nécessaires pour le matériel utilisé. Le programme linuxrc vous assiste lors du chargement des modules de noyau prenant en charge votre matériel et démarre ensuite l'installation.

3.5.1 Créer une disquette d'amorçage avec rawwritewin

Sous Windows, il est possible de créer des disquettes d'amorçage grâce au programme graphique rawwritewin. Vous trouverez ce programme sur le CD 1 dans le répertoire `dosutils/rawwritewin`.

Une fois démarré, vous devez lui indiquer le fichier image. Les fichiers images se trouvent sur le CD 1 dans le répertoire `boot`. Au minimum vous avez besoin des images `bootdisk` et `modules1`. Pour voir ces fichiers dans l'explorateur de fichiers, vous devez changer le type de fichier en `all files` (tous les fichiers). Insérez alors une disquette dans votre lecteur de disquettes et cliquez sur 'Write'.

Vous pouvez aussi créer de cette manière les autres images de disquettes `modules1`, `modules2`, `modules3` et `modules4`. Celles-ci sont nécessaires lorsque vous avez des périphériques USB ou SCSI ou une carte réseau ou PCMCIA et que vous souhaitez y accéder dès l'installation. Une disquette de modules peut aussi s'avérer nécessaire pour utiliser un système de fichiers spécial au cours de cette phase.

3.5.2 Créer une disquette d'amorçage avec rawrite

Pour créer les disquettes d'amorçage et de modules de SUSE, vous disposez du programme DOS `rawrite.exe` (CD 1, répertoire `dosutils\rawrite`). Un ordinateur équipé d'un DOS (par exemple FreeDOS) ou de Windows est nécessaire pour cette opération.

Voici la description des étapes si vous travaillez sous Windows XP :

1. Insérez le CD numéro 1 de SUSE LINUX.
2. Ouvrez une fenêtre DOS (avec le menu 'Démarrer', dans 'Utilitaires' → 'Invite de commandes MS-DOS').
3. Démarrez le programme rawrite.exe en indiquant le chemin correct vers le lecteur de CD. Dans notre exemple, vous vous trouvez sur le disque dur `C:`, dans le répertoire `Windows` et votre lecteur de CD porte la lettre `D:`.

   ```
   d:\dosutils\rawrite\rawrite
   ```

4. Après avoir démarré, le programme demande la source et la cible (destination) du fichier à copier. Il s'agit de l'emplacement de l'image de la disquette d'amorçage sur le CD 1 qui se trouve dans le répertoire `boot`. Le nom du fichier est `bootdisk`. N'oubliez pas non plus d'indiquer ici le chemin vers votre lecteur de CD.

   ```
   d:\dosutils\rawrite\rawrite
   RaWrite 1.2 - Write disk file to raw floppy diskette

   Enter source filename: d:\boot\bootdisk
   Enter destination drive: a:
   ```

Dès que vous avez saisi la lettre du lecteur cible `a:`, rawrite vous invite à insérer une disquette formatée et à appuyer sur Entrée. La progression de la copie s'affiche ensuite. La procédure peut être interrompue à l'aide de la combinaison de touches Ctrl-C. Pour créer plusieurs disquettes, répétez la même procédure.

3.5.3 Créer une disquette d'amorçage sous un système de type UNIX

Sur un système UNIX ou Linux, vous avez besoin d'un lecteur de CD-ROM et de plusieurs disquettes formatées. Pour créer des disquettes d'amorçage, procédez comme suit :

1. Si vous devez d'abord formater les disquettes :

   ```
   fdformat /dev/fd0u1440
   ```

   Cette commande vérifie également que la disquette ne contient pas d'erreur. N'utilisez pas un support avec des erreurs.

2. Insérez le CD 1 dans votre lecteur de CD-ROM et placez-vous dans le répertoire `boot` sur le CD : sur les versions actuelles de SUSE vous n'avez plus besoin de monter le CD.

   ```
   cd /media/cdrom/boot
   ```

3. Créez la disquette d'amorçage avec la commande

   ```
   dd if=bootdsk1 of=/dev/fd0 bs=8k
   ```

4. Répétez la procédure avec les images `bootdsk2` et `bootdsk3`.

Dans le répertoire `boot`, le fichier `README` vous indique les détails concernant les images de disquettes; ces fichiers se lisent avec `more` ou `less`.

Les autres images de disquettes (`modules1`, `modules2`, `modules3` et `modules4`) peuveut être crées de la même manière. Ces disquettes sont nécessaires si vous avez des périphériques USB ou SCSI ou une carte réseau ou PCMCIA que vous souhaitez utiliser au cours de l'installation. Un disque de module peut aussi s'avérer nécessaire pour utiliser un système de fichiers particulier pendant l'installation.

La création de disques de module n'est pas évidente. Vous trouverez une description détaillée de la méthode de création d'un disque de module dans `/usr/share/doc/packages/yast2-installation/vendor.html`.

3.5.4 Amorcer depuis une disquette (SYSLINUX)

La disquette d'amorçage est utilisée pour gérer des cas particuliers d'installation (par exemple s'il n'y a pas de lecteur de CD-ROM disponible). Le processus d'amorçage est déclenché par le chargeur d'amorçage Syslinux (paquetage `syslinux`). Syslinux est configuré de manière à effectuer une reconnaissance du matériel limitée lors de l'amorçage. Il s'agit essentiellement des étapes suivantes :

1. Le programme vérifie si le BIOS prend en charge un framebuffer conforme à VESA 2.0 et amorce le noyau en conséquence.
2. Les données des moniteurs (informations DDC) sont lues.
3. Lire le bloc numéro 1 depuis le premier disque dur (MBR) pour décider plus tard de d'attribuer des identificateurs BIOS aux noms des périphériques (devices) lors de la configuration du gestionnaire d'amorçage. Il faut en outre essayer de lire le bloc au moyen des fonctions lba32 du BIOS pour vérifier s'il gère ces fonctions.

Astuce

Pour ignorer toutes ces étapes, il suffit de maintenir la touche Maj appuyée au démarrage de Syslinux. En cas d'erreur, ajoutez la ligne

```
verbose 1
```

dans `syslinux.cfg`. Le gestionnaire d'amorçage annonce alors chaque action en cours.

Astuce

Si l'ordinateur refuse de s'amorcer depuis la disquette, il est probable qu'il faille auparavant adapter la séquence d'amorçage dans le BIOS ainsi : `A,C,CDROM`.

► **x86**

Sur les systèmes x86, outre le CD 1, le deuxième CD est également amorçable. Tandis que le CD 1 fonctionne grâce à une image ISO amorçable, le CD 2 est amorcé au moyen d'une image de disquette de 2,88 Mo. N'utilisez le CD 2 que si vous êtes sûr que vous pouvez amorcer depuis un CD, mais que cela ne fonctionne pas avec le CD 1 (c'est une solution de repli). ◄

3.5.5 Lecteurs de CD-ROM non pris en charge

La plupart des lecteurs de CD-ROM sont pris en charge. Si des problèmes surviennent lorsque l'on amorce depuis le lecteur de CD-ROM, essayez d'amorcer le CD 2 de l'ensemble de CD fourni.

Si le système ne possède ni lecteur de CD-ROM ni lecteur de disquette, il est encore possible d'utiliser un CD-ROM externe, connecté en USB, FireWire ou SCSI pour amorcer le système. Cela dépend fortement de l'interaction entre le BIOS et le matériel utilisé. Une mise à jour du BIOS peut parfois vous aider si vous rencontrez des difficultés.

3.5.6 Installation depuis une source dans le réseau

Parfois, l'installation par défaut au moyen d'un lecteur de CD-ROM n'est pas possible. Par exemple, votre lecteur de CD-ROM peut ne pas être pris en charge du fait qu'il s'agit d'un ancien lecteur propriétaire. Ou bien votre second ordinateur, par exemple un portable, n'a peut-être pas de lecteur de CD-ROM mais uniquement un adaptateur Ethernet. SUSE LINUX vous permet de procéder à une

installation sur des machines sans lecteur CD-ROM via une connexion réseau. En règle générale, on utilise NFS ou FTP via ethernet.

Cette méthode n'est pas couverte par l'assistance à l'installation. Elle est donc réservée aux seuls utilisateurs expérimentés.

Pour installer SUSE LINUX depuis une source réseau, deux étapes sont nécessaires :

1. La mise à disposition des données nécessaires à l'installation (CD, DVD) sur un ordinateur qui servira plus tard de source d'installation.
2. Le système à installer doit être amorcé depuis une disquette, un CD ou le réseau et celui-ci doit être configuré.

La source d'installation peut être rendue disponible via divers protocoles tels que NFS et FTP. Consultez la section 3.1.1 page 92 pour plus d'informations relatives à l'installation en question.

3.6 Associer des noms de fichiers de périphériques permanents aux périphériques SCSI

Les périphériques SCSI reçoivent lors de l'amorçage des noms de fichiers de périphérique qui leur sont attribués de manière plus ou moins dynamique. Ceci n'est pas un problème tant que ni le nombre ni la configuration des périphériques ne sont modifiés. Mais lorsque l'on ajoute un disque dur SCSI supplémentaire, et que celui-ci est reconnu par le noyau avant l'ancien disque dur, ce dernier reçoit un nouveau nom et la déclaration dans la table de montage `/etc/fstab` ne correspond pas.

Pour contourner cette difficulté, il est possible d'utiliser le script d'amorçage du système `boot.scsidev`. Activez ce script à l'aide de la commande `/sbin/insserv` et réglez les paramètres nécessaires dans `/etc/sysconfig/scsidev`. Le script `/etc/rc.d/boot.scsidev` assure la configuration des périphériques SCSI au cours de la procédure d'amorçage et inscrit des noms de périphériques permanents dans `/dev/scsi/`. Ces noms de périphériques peuvent ensuite être utilisés dans `/etc/fstab`. De plus, il est possible de définir des noms de périphériques persistants pour la configuration SCSI dans

/etc/scsi.alias. Le schéma d'attribution de nom des périphériques dans /etc/scsi est expliqué dans man scsidev

Dans le mode expert de l'éditeur de niveaux d'exécution, il faut faire appel à boot.scsidev pour l'étape B, les liens utiles sont alors placés dans /etc/init.d/boot.d, ce qui permet de créer les noms lors de l'amorçage.

Astuce

Noms de périphériques et udev

boot.scsidev est également pris en charge sous SUSE LINUX. Cependant, il est conseillé pour créer des noms de périphériques permanents d'utiliser udev pour créer des noms de périphériques permanents dans /dev/by-id/.

Astuce

3.7 Configuration du gestionnaire de volumes logiques (LVM)

Cette section décrit brièvement les principes sous-jacents à LVM et ses fonctions de base qui le rendent utile dans de nombreuses circonstances. Vous apprendrez dans la section 3.7.2 page 107 à paramétrer LVM avec YaST.

Avertissement

Utiliser LVM peut augmenter les risques de perdre des données. Mais les risques informatiques comprennent aussi les applications qui échouent, les pannes de courant et les commandes erronées. Sauvegardez vos données avant de mettre en place LVM ou de reconfigurer les volumes. Ne travaillez jamais sans sauvegarde.

Avertissement

3.7.1 Le gestionnaire de volumes logiques

Le gestionnaire de volumes logiques (LVM) permet de répartir de manière flexible la place sur le disque dur entre différents systèmes de fichiers. Il a été développé car il est parfois nécessaire de modifier la répartition de l'espace disque

après que le partitionnement initial a déjà été fait pendant l’installation. Comme il est difficile de modifier des partitions sur un système en cours d’exploitation, LVM fournit une réserve virtuelle d’espace disque (groupe de volumes, en abrégé VG) dans lequel des volumes logiques (LV)sont créés en fonction des besoins. Le système d’exploitation utilise alors ces derniers plutôt que les partitions physiques. Les groupes de volumes peuvent s’étendre sur plus d’un disque de manière à ce que plusieurs disques ou parties de disque puissent constituer un seul VG. LVM présente ainsi une certaine abstraction par rapport à l’espace disque physique qui permet de modifier sa répartition d’une manière bien plus simple et sûre qu’en repartitionnant physiquement. Vous trouverez des informations sur le partitionnement physique dans la section Types de partition page 12 et dans la section 2.7.5 page 75.

FIG. 3.1: *LVM par rapport au partitionnement physique*

La figure 3.1 de la présente page compare un partitionnement physique (à gauche) et une segmentation LVM (à droite). À gauche, un unique disque a été divisé en trois partitions physiques (PART), chacune avec un point de montage (PM) attribué de manière à ce que le système d’exploitation puisse y accéder. À droite, deux disques ont été divisés en respectivement deux et trois partitions physiques. Deux volumes LVM (VG 1 et VG 2) ont été définis. VG 1 contient deux partitions du DISQUE 1 et une du DISQUE 2. VG 2 contient les deux partitions restantes du DISQUE 2. Dans LVM, les partitions de disque physiques incorporées dans un groupe de volume sont appelées volumes physiques (PV). Dans les groupes de volumes, quatre volumes logiques (LV 1 à LV 4) ont été définis et peuvent être utilisés par le système d’exploitation par le biais des points de mon-

tages associés. Les frontières entre les différents volumes logiques ne sont pas nécessairement alignées avec les frontières de partitions. Voir la frontière entre LV 1 et LV 2 dans cet exemple.

Fonctionnalités de LVM :

- Vous pouvez rassembler plusieurs disques durs ou partitions en un grand volume logique.
- Si l'espace disponible sur un volume logique (par exemple `/usr`) tire à sa fin, vous pouvez l'agrandir en le configurant de manière appropriée.
- Avec le gestionnaire de volumes logiques, vous pouvez même ajouter des disques durs ou des volumes logiques dans un système en cours d'exploitation ; la condition préalable étant qu'il faut utiliser du matériel pouvant être remplacé à chaud approprié pour ce genre d'interventions.
- On peut activer un "mode d'entrelacement" (striping mode) qui distribue le flux de données d'un volume logique sur plusieurs volumes physiques. Si ces volumes physiques se situent sur des disques différents, ceci peut améliorer les performances en lecture et en écriture de la même manière que RAID 0.
- La fonctionnalité de "snapshot" (instantané) permet, notamment sur les serveurs, de réaliser des sauvegardes cohérentes alors même que le système est en cours de fonctionnement.

Ces fonctionnalités rendent déjà l'utilisation de LVM pertinente pour des ordinateurs domestiques très utilisés ou pour des petits serveurs. Si vous avez un volume de données en évolution constante comme des bases de données, des archives de musique ou des répertoires utilisateur, LVM est exactement ce qu'il vous faut. Ceci vos permet d'avoir des systèmes de fichiers plus grands que le disque dur physique. Un autre avantage de LVM est que vous pouvez créer jusque 256 volumes logiques. Gardez cependant à l'esprit que le travail avec LVM est différent du travail avec des partitions classiques. Vous trouverez des instructions et des informations supplémentaires sur la configuration des LVM dans le guide pratique officiel de LVM à l'adresse `http://www.traduc.org/docs/HOWTO/lecture/LVM-HOWTO.html`

À partir de la version 2.6 du noyau, la version 2 de LVM est disponible. Elle assure la compatibilité descendante avec la version précédente de LVM et peut toujours gérer les anciens groupes de volumes. Lorsque vous créez de nouveaux groupes de volumes, vous devez décider si vous voulez utiliser le nouveau format ou la version avec compatibilité descendante. LVM 2 ne nécessite aucun correctif du noyau. Il utilise la mise en correspondance des périphériques (device mapper) intégrée au noyau 2.6. Ce noyau ne prend en charge que la version 2 de LVM. C'est pourquoi lorsque nous parlerons de LVM dans cette section nous nous référerons toujours à LVM dans sa version 2.

3.7.2 Configuration du gestionnaire de volumes logiques avec YaST

Vous pouvez accéder à la configuration de LVM avec YaST par le biais du partitionnement en mode expert (voir la section 2.7.5 page 75). Cet outil de partitionnement professionnel vous permet de modifier et de supprimer les partitions existantes et d'en créer de nouvelles qui peuvent être utilisées avec LVM. Vous pouvez y créer une partition LVM en cliquant d'abord sur 'Créer' → 'Ne pas formater' puis en choisissant '0x8E Linux LVM' comme identifiant de partition. Après avoir créé toutes les partitions à utiliser avec LVM, cliquez sur 'LVM' pour commencer à configurer LVM.

Créer des groupes de volumes

Si aucun groupe de volumes n'existe encore sur votre système, on vous demande d'en ajouter un (voir la figure 3.2 page suivante). On peut créer des groupes supplémentaires avec 'Ajouter groupe' mais un seul groupe de volumes est généralement suffisant. Le nom `system` est suggéré pour le groupe de volumes dans lequel se trouvent les fichiers système de SUSE LINUX. La taille des extensions physiques définit la taille d'un bloc physique dans le groupe de volumes. Tout l'espace disque d'un groupe de volumes est géré en morceaux de cette taille. Cette valeur est normalement définie à 4 Mo et permet une taille maximale de 256 Go pour les volumes physiques et logiques. La taille des extensions physiques ne devrait être augmentée par exemple à 8, 16 ou 32 Mo si vous avez besoin de volumes plus gros que 256 Go.

Configuration des volumes physiques

Lorsque vous avez créé un groupe de volumes, la boîtes de dialogue suivantes donnent la liste de toutes les partitions qui possèdent le type "Linux LVM" ou "Linux native". Aucune partition d'échange ou DOS n'est affichée. Si une partition est déjà attribuée à un groupe de volumes, c'est le nom du groupe de volumes qui est affiché dans la liste. Les partitions non attribuées sont identifiées par "--".

Si vous utilisez plusieurs groupes de volumes, choisissez le groupe de volumes courant dans la boîte de sélection en haut à gauche. Utilisez les boutons en haut à droite pour créer des groupes de volumes supplémentaires et supprimer des groupes de volumes existants. Vous ne pouvez cependant supprimer que les groupes de volumes auxquels plus aucune partition n'est attribuée. Toutes les

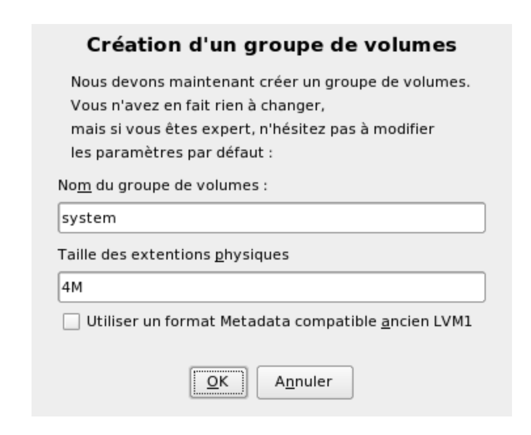


FIG. 3.2: *Créer un groupe de volumes*

partitions attribuées à un groupe de volumes sont également appelées volumes physiques (Physical Volume, PV).

Pour ajouter dans le groupe de volumes de votre choix une partition jusqu'alors non attribuée, cliquez d'abord sur la partition, puis sur le bouton 'Ajouter volume'. Le nom du groupe de volumes est alors placé à côté de la partition sélectionnée. Nous vous conseillons d'attribuer toutes les partitions que vous envisagez d'utiliser pour le gestionnaire de volumes logiques à un groupe de volumes sans quoi l'espace de la partition reste inutilisé. Avant de pouvoir quitter la boîte de dialogue, un volume physique au moins doit être attribué à chaque groupe de volumes. Après avoir attribué tous les volumes physiques, cliquez sur 'Suivant' pour configurerles volumes logiques.

Configurer les volumes logiques

Une fois que le groupe de volumes a été rempli avec des volumes physiques, définissez dans la boîte de dialogue suivante les volumes logiques que le système d'exploitation doit utiliser. Choisissez le groupe de volumes courant dans la boîte de sélection en haut à gauche. L'espace disponible dans le groupe de volume courant est affiché à côté. La liste en-dessous contient tous les volumes logiques de ce groupe de volumes. Toutes les partitions Linux normales auxquelles est associé un point de montage, toutes les partitions d'échange et les volumes logiques déjà existants y sont listés. Vous pouvez 'Ajouter', 'Modifier' et 'Supprimer' des

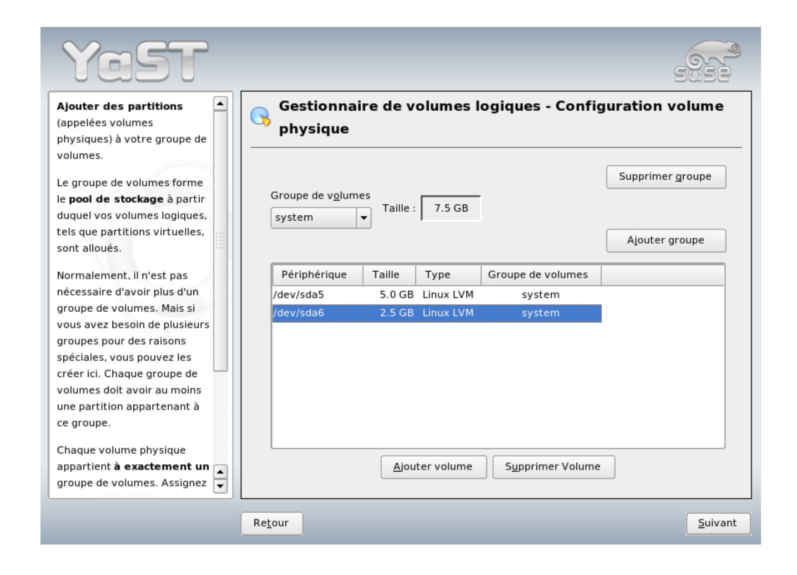


FIG. 3.3: *Paramétrage des volumes physiques*

volumes logiques à votre convenance jusqu'à ce que tout l'espace du groupe de volume soit utilisé. Associez au moins un volume logique à chaque groupe de volumes.

Pour créer un nouveau volume logique, cliquez sur 'Ajouter' et remplissez la fenêtre qui s'ouvre. La taille, le système de fichiers et le point de montage peuvent être saisis comme pour le partitionnement. Normalement vous créez un système de fichiers comme reiserfs ou ext2 sur le volume logique et vous lui affectez un point de montage. Les fichiers enregistrés sur ce volume logique se trouvent à ce point de montage sur le système installé. Il est de plus possible de distribuer le flux de données des volumes logiques sur plusieurs volumes physiques (entrelacement ou striping). Si ces volumes physiques se situent sur des disques durs distincts, cela implique en général de meilleurs performances en lecture et en écriture (comme en RAID 0). Cependant, un LV réparti en n tranches ne peut être créé correctement que si l'espace disque requis par le LV peut être distribué de manière homogène entre n volumes physiques. Si seuls deux volumes physiques sont disponibles, il est impossible de répartir un volume logique en trois tranches.

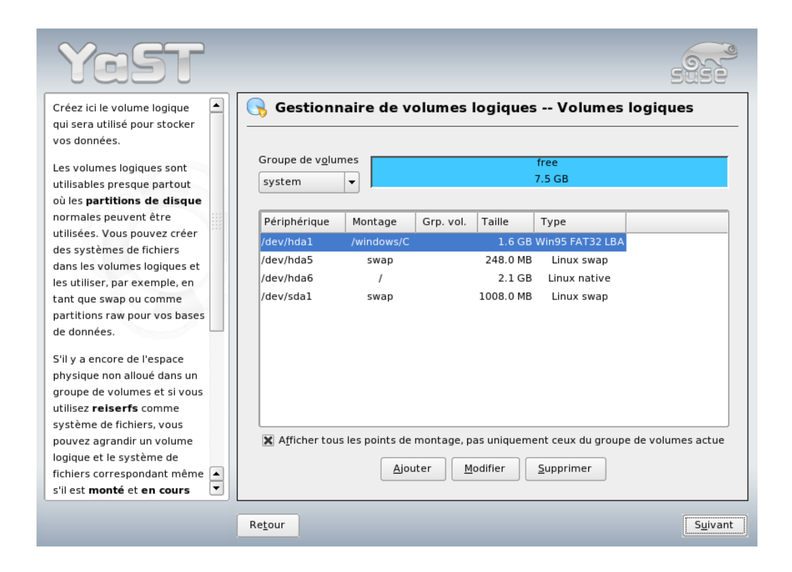


FIG. 3.4: *Gestion des volumes logiques*

Avertissement

Entrelacement

YaST n'est pas capable à ce moment de vérifier que vos déclarations concernant l'entrelacement sont correctes. Une erreur sur ce point n'apparaît que plus tard lorsque LVM est mis en place sur le disque.

Avertissement

Si vous aviez déjà configuré LVM sur votre système, les volumes logiques existants apparaissent ici. Avant de continuez, associez les points de montage appropriés à ces volumes logiques. Retournez au partitionnement en mode expert de YaST avec 'Suivant' et terminez-y votre travail.

Gestion directe du LVM

Si vous avez déjà configuré LVM et si vous ne voulez qu'effectuer des modifications,il existe une méthode alternative. Dans le Centre de Contrôle de YaST, choisissez 'Système' → 'Partitionnement'.



FIG. 3.5: *Créer des volumes logiques*

Cette boîte de dialogue propose à peu près les actions décrites ci-dessus à l'exception du partitionnement physique. Elle montre les volumes physiques et logiques existants dans deux listes et vous pouvez gérer votre système LVM selon les méthodes décrites précédemment.

3.8 Configuration RAID logiciel

La technologie RAID (réseau redondant de disques indépendants, en anglais Redundant Array of Independent Disks) repose sur l'idée de rassembler plusieurs partitions de disque dur en un seul gros disque *virtuel* afin d'optimiser les performances et la sûreté des données, chacune de ces exigences étant exclusive de l'autre. Un contrôleur RAID utilise généralement le protocole SCSI, qui permet de mieux contrôler un plus grand nombre de disques durs que le protocole IDE et qui se prête mieux au traitement des commandes en parallèle. Entre-temps, il

existe également des contrôleurs RAID qui fonctionnent avec des disques durs IDE ou SATA. À ce sujet, consultez également la base de données matériel sous `http://cdb.suse.de`.

3.8.1 RAID logiciel

Le contrôleur RAID, qui peut être un équipement très coûteux, peut être avantageusement remplacé par le RAID logiciel, qui est capable de remplir les mêmes fonctions. SUSE LINUX vous offre la possibilité, en utilisant YaST, de combiner plusieurs disques durs en un système RAID logiciel ce qui constitue une alternative très avantageuse au RAID matériel. RAID implique diverses stratégies pour combiner plusieurs disques durs dans un système RAID, chacunde de ces stratégies ayant des objectifs, des avantages et des caractéristiques différents. Ces variations sont connues comme des *niveaux RAID*.

Les niveaux RAID courants sont :

RAID 0 Ce niveau améliore les performances de vos accès aux données en distribuant des blocs de chaque fichier à travers de multiples disques. Il ne s'agit pas, à proprement parler, de RAID véritable, en raison de l'absence de sauvegarde des données. Malgré cela, le terme "RAID 0" est entré dans l'usage pour ce genre de système. Le "RAID 0" combine au moins deux disques durs. Les performances sont très bonnes mais il suffit qu'un seul des disques, quel qu'en soit le nombre, soit défaillant pour que le système RAID soit détruit, entraînant la perte de vos données.

RAID 1 Ce niveau offre une sûreté des données satisfaisante, celles-ci étant copiées dans un rapport 1:1 sur un autre disque dur, selon la technique de *mise en miroir de disques durs*. Dans le cas où un disque viendrait à être détruit, une copie de son contenu se trouve sur un autre disque. Tous les disques sauf un peuvent donc être défectueux sans risque de perte de données. Les performances en écriture diminuent quelque peu en comparaison à l'accès monodisque (on constate un ralentissement de l'ordre de 10 à 20 %). En contrepartie, les performances en lecture représentent une nette amélioration par rapport à l'utilisation d'un unique disque dur physique normal. En effet, les données sont dupliquées et peuvent donc être lues en parallèle. En règle générale, on peut dire que le niveau 1 offre une vitesse de lecture deux fois plus importantes que les monodisques pour pratiquement la même vitesse en écriture.

RAID 2 et RAID 3 Il ne s'agit pas d'impleméntations RAID typiques. Le niveau 2 segmente les données au niveau du bit plutôt qu'au niveau du bloc. Le niveau 3 répartit les données au niveau du bit sur plusieurs disques en dédiant un disque à la parité et ne peut pas répondre à de multiples requêtes simultanées. Ces deux niveaux ne sont que rarement utilisés.

RAID 4 Le niveau 4 offre une distribution des blocs de données comme le niveau 0 combinée avec un disque dédié à la parité. En cas de disque de données défectueux, les données de parité sont utilisées pour créer un disque de remplacement. Cependant, le disque de parité peut ralentir considérablement l'accès en écriture. Néanmoins, le niveau 4 est parfois utilisé.

RAID 5 Le niveau RAID 5 est un compromis optimal entre le niveau 0 et le niveau 1 en ce qui concerne la redondance et les performances. L'espace disque disponible correspond au nombre de disques utilisés moins un. Comme dans le niveau RAID 0, les données sont réparties entre les disques. La sécurisation des données est dévolue à des *blocs de parité* qui sont créés sur l'une des partitions. Ceux-ci sont combinés par XOR, ce qui permet, en cas de défaillance d'une partition, d'utiliser le bloc de parité correspondant pour reconstituer le contenu avec l'aide de l'opération logique XOR. Le RAID 5 ne permet pas d'avoir plus d'un disque dur défaillant à la fois. Dès qu'un disque dur est hors service, il doit être remplacé le plus vite possible afin d'éviter de perdre les données.

Autres niveaux RAID Plusieurs autres niveaux RAID ont été développés (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50, etc.) ; certains sont des implémentations propriétaires créées par des fabricants de matériel. Ces niveaux ne sont pas très répandus et ne sont donc pas expliqués ici.

3.8.2 Configuration du RAID logiciel avec YaST

La configuration du RAID logiciel est accessible depuis le partitionneur expert de YaST (voir la section 2.7.5 page 75). Cet outil de partitionnement professionnel vous permet de modifier et d'effacer des partitions existantes et d'en créer de nouvelles à utiliser avec RAID logiciel. Créez des partitions RAID en cliquant sur 'Créer' → 'Ne pas formater' puis en sélectionnant '0xFD Linux RAID' comme identificateur de partition. Les niveaux RAID 0 et RAID 1 requièrent au moins deux partitions—elles sont normalement au nombre de deux exactement pour le RAID 1. En revanche, le RAID 5 requiert au moins trois partitions. Il est recommandé de n'utiliser que des partitions de taille identique. Les différentes partitions d'un RAID doivent être installées sur différents disques durs afin de parer

au risque de perte de données dû à la défaillance d'un disque dur (RAID 1 et 5) et pour optimiser les performances en RAID 0. Après avoir créé toutes les partitions à utiliser avec RAID, cliquez sur 'RAID' → 'Créer RAID' pour démarrer la configuration RAID.

Dans le dialogue suivant, choisissez entre les niveaux RAID 0, 1 et 5 (voir la section 3.8.1 page 112 pour plus de détails). Après avoir cliqué sur 'Suivant', le dialogue suivant vous donne une liste de toutes les partitions avec le type "Linux RAID" ou "Linux native" (voir la figure 3.6 de la présente page). Aucune partition swap ou DOS n'est montrée. Si une partition est déjà attribuée à un volume RAID, le nom du périphérique RAID (par exemple, `/dev/md0`) est indiqué dans la liste. Les partitions non attribuées sont marquées avec "--".

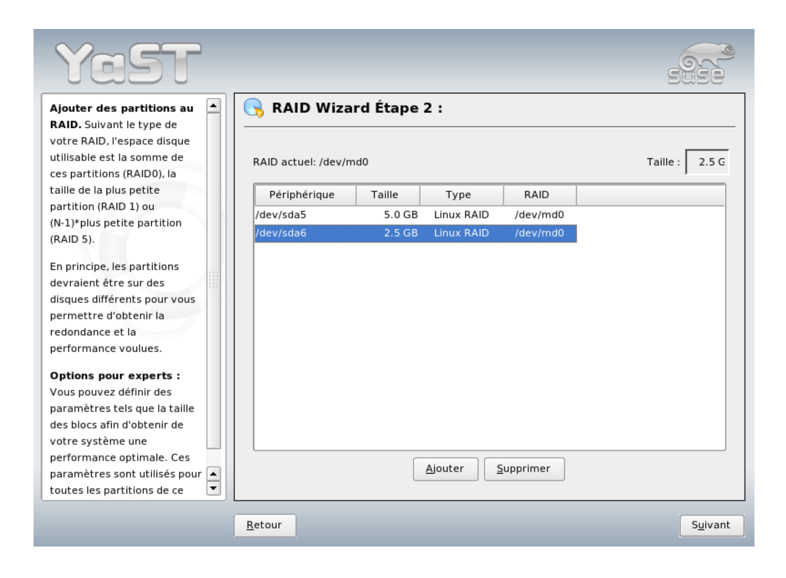


FIG. 3.6: *Partitions RAID*

Pour ajouter une partition non encore attribuée au volume RAID sélectionné, cliquez sur la partition puis sur 'Ajouter'. À cet instant, le nom du périphérique RAID est entré en face de la partition sélectionnée. Attribuez toutes les partitions réservées pour RAID. Dans le cas contraire, l'espace sur les partitions non attribuées restera inutilisé. Après avoir attribué toutes les partitions, cliquez sur 'Suivant' pour passer au dialogue de configuration où vous pourrez procéder au réglage fin de la performance (voir la figure 3.7 page suivante).

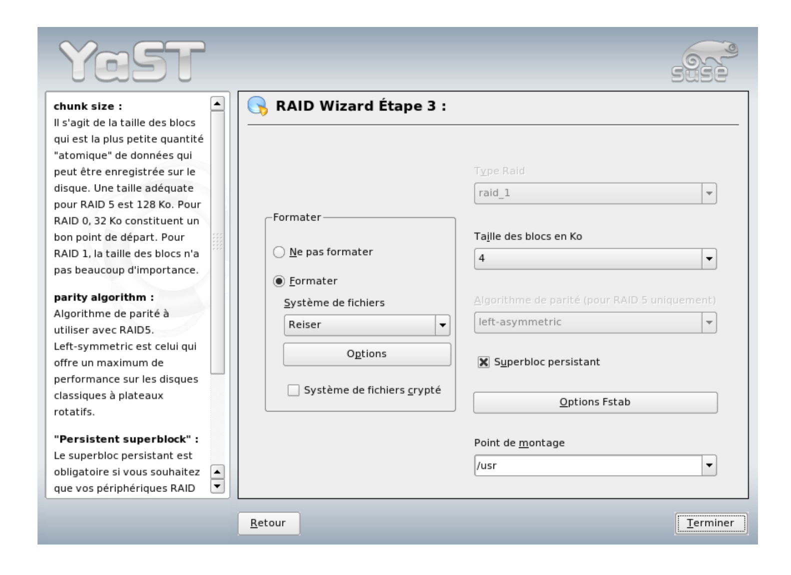


FIG. 3.7: *Paramètres du système de fichiers*

Comme dans le cas du partitionnement conventionnel, configurez le système de fichiers de façon à utiliser ainsi que le chiffrement et le point de montage pour le volume RAID. Lorsque la case ‘superbloc permanent’ est cochée, les partitions RAID seront reconnues en tant que telles juste lors de l’amorçage de l’ordinateur. Après avoir accepté la configuration en cliquant sur ‘Terminer’, vous voyez le périphérique `/dev/md0` et d’autres assorti de l’identifiant *RAID* dans le l’outil de partitionnement pour expert.

3.8.3 Troubleshooting

Pour savoir si une partition RAID est déteriorée, examinez le contenu du fichier `/proc/mdstats`. La procédure à suivre lorsqu’un dysfonctionnement s’est produit, est d’arrêter votre système Linux et de remplacer le disque défectueux par un nouveau disque partitionné de manière identique. Redémarrez ensuite votre système et exécutez la commande `mdadm /dev/mdX --add /dev/sdX`. Bien entendu, vous devez remplacer ’X’ par les identificateurs spécifiques à vos périphériques. Le nouveau disque dur est alors automatiquement intégré au système RAID et est totalement restauré.

3.8.4 Informations complémentaires

Vous trouverez les instructions pour la configuration et plus de détails au sujet de RAID logiciel dans les HOWTO sous :

- /usr/share/doc/packages/raidtools/Software-RAID.HOWTO.html
- http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html

Des listes de diffusion Linux RAID sont également disponibles, par exemple http://www.mail-archive.com/linux-raid@vger.rutgers.edu.

Mise à jour du système et gestion des paquetages

SUSE LINUX offre la possibilité de mettre à jour un système existant sans le réinstaller complètement. Cependant, il faut faire une distinction entre l'*actualisation de divers paquetages logiciels* et une *mise à jour de l'ensemble du système*. Vous pouvez aussi installer divers paquetages à la main avec le gestionnaire de paquetages rpm.

4.1 Mise à jour de SUSE LINUX

Il est bien connu que les logiciels ”grossissent“ d'une version à l'autre. Par conséquent, il convient de vérifier avec `df` la capacité maximale des différentes partitions avant la mise à jour. Si vous estimez que l'espace risque d'être limité, faites alors une sauvegarde de vos données avant la mise à jour et partitionnez le système à nouveau. Il n'est pas possible de donner à chacun des règles générales quant à la quantité d'espace nécessaire. L'espace requis dépend du type de partitionnement existant, des logiciels choisis et du numéro de version de SUSE LINUX.

Important

Nous ne saurions trop vous recommander de lire sur le CD le fichier `README` ou sous DOS ou Windows, le fichier `README.DOS`. Ce fichier contient toutes les modifications qui ont eu lieu après l'impression de ce manuel.

Important

4.1.1 Préparatifs

Avant le début d'une mise à jour, il est plus sûr de copier les anciens fichiers de configuration sur un support séparé, tel qu'un dévideur à bande ou streamer, un disque dur amovible, un lecteur de disquettes ZIP. Il s'agit principalement des fichiers enregistrés dans `/etc` ainsi que certains des répertoires et fichiers présents dans `/var` et dans `/opt`. En outre, il peut être utile de sauvegarder les données actuelles des utilisateurs contenues dans `/home` (les répertoires personnels contenus dans `HOME`) sur un support tiers. La sauvegarde des données doit se faire que `root`. Seul `root` dispose des droits permettant de lire tous les fichiers locaux.

Avant de commencer la procédure de mise à jour, notez l'emplacement de la partition racine ; la commande `df /` vous permet de connaître le nom du périphérique abritant la partition racine. Dans l'exemple 4.1 de la présente page, la partition racine à noter est `/dev/hda2` (montée comme `/`).

Example 4.1: *Aperçu avec* `df -h`

```
Sys. de fich. Tail. Occ. Disp. %Occ. Monté sur
/dev/hda1     1,9G  189M  1,7G  10% /dos
/dev/hda2     8,9G  7,1G  1,4G  84% /
/dev/hda5     9,5G  8,3G  829M  92% /home
```

4.1.2 Problèmes possibles

Contrôler passwd et group dans /etc

Avant la mise à jour, assurez-vous que /etc/passwd et /etc/group ne comportent pas d'erreur de syntaxe. À cette fin, exécutez les programmes de vérification pwck et grpck en tant que root et corrigez les erreurs qui ont été signalées.

PostgreSQL

Avant une mise à jour de PostgreSQL (postgres) , il est généralement recommandé d'exporter (dump) les bases de données. Consultez la page de manuel de pg_dump. Cette opération n'est nécessaire que si vous avez effectivement utilisé PostgreSQL avant la mise à jour.

4.1.3 Mise à jour avec YaST

Après les travaux préliminaires décrits dans la section 4.1.1 page précédente, vous pouvez procéder à la mise à jour de votre système :

1. Démarrez le système comme décrit dans la section 1.1 page 4 pour une installation. Dans YaST, après avoir défini la langue, sélectionnez 'Mise à jour d'un système existant'. Ne sélectionnez pas 'Nouvelle installation'.
2. YaST détermine s'il existe plus d'une partition racine. S'il n'y en a qu'une, passez à l'étape suivante. S'il existe plusieurs partitions, choisissez celle qui convient et confirmez par 'Suivant' (la partition /dev/hda2 a été sélectionnée dans l'exemple de la section 4.1.1 page précédente). YaST lit l'ancien fichier fstab présent sur cette partition pour ensuite analyser les systèmes de fichiers qui y sont répertoriés et enfin les monter.
3. Vous avez alors la possibilité de créer une copie de sauvegarde des fichiers système pendant la mise à jour. Cette option ralentit la procédure de mise à jour, mais vous devriez la choisir si vous n'avez pas de sauvegarde système récente.
4. Dans la boîte de dialogue suivante, choisissez soit de ne mettre à jour que les logiciels déjà installés, soit d'ajouter des nouveaux composants logiciels au système (mode de mise à niveau). Il est recommandé d'accepter la proposition qui vous est faite, par exemple le 'Système par défaut'. Vous pourrez ajuster les détails plus tard à l'aide de YaST.

4.1.4 Mise à jour individuelle des paquetages

Indépendamment d'une mise à jour complète, vous pouvez actualiser à tout moment les différents paquetages. Vous devrez toutefois veiller *vous-même* à ce que le système reste cohérent : vous trouverez des recommandations de mise à jour à l'adresse `http://www.novell.com/linux/download/updates/`.

Dans le menu de sélection de paquetages de YaST, vous pouvez sélectionner tous les composants dont vous avez besoin. Si vous choisissez de mettre à jour un paquetage qui joue un rôle fondamental dans le fonctionnement du système, YaST vous en avertit. Les paquetages de ce type ne devraient être actualisés qu'en mode de mise à jour. Par exemple, quelques paquetages contiennent des *bibliothèques partagées*, potentiellement utilisées au moment de la mise à jour. Une mise à jour dans le système actuel en fonctionnement amènerait donc ces programmes à ne plus pouvoir fonctionner correctement.

4.2 Modifications des logiciels d'une version à l'autre

Les sections suivantes dressent la liste des détails qui ont changé d'une version à l'autre. Cet aperçu montre si des configurations ont été modifiées, si des fichiers de configuration ont été déplacés ou encore, si des applications connues ont été modifiées de façon significatives. Il ne sera traité que des aspects qui affectent directement l'utilisateur ou l'administrateur dans leur travail quotidien.

Les problèmes et les particularités de chaque version sont mis en ligne dès qu'ils sont connus : voyez les liens ci-dessous. On peut accéder aux mises à jour importantes des différents paquetages à l'adresse `http://www.novell.com/products/linuxprofessional/downloads/` en utilisant YaST Online Update (YOU)—voir la section 2.2.3 page 50.

4.2.1 De la version 8.1 à la version 8.2

Problèmes et particularités : `http://portal.suse.com/sdb/en/2003/04/bugs82.html` (en anglais).

- Prise en charge 3D des cartes graphiques de type nVidia (modifications) : les paquetages `NVIDIA_GLX/NVIDIA_kernel` (y compris le script

switch2nvidia_glx) ne sont plus fournis. Téléchargez le programme d'installation nVidia pour Linux IA32 sur la page web de nVidia (http://www.nvidia.com), utilisez-le pour installer le pilote, puis faites appel à SaX2 ou à YaST pour activer la prise en charge 3D.

- Lors d'une nouvelle installation, le démon xinetd est installé à la place du démon inetd et configuré avec des valeurs sûres. Voyez le répertoire /etc/xinetd.d. Néanmoins, le démon inetd reste tout de même en place lors d'une mise à jour du système.
- PostgreSQL est disponible dans sa version 7.3. Un *dump/restore* (export/import des données) est effectué avec pg_dump pour une mise à jour depuis une version 7.2.x. Lorsque votre application interroge les catalogues système, d'autres adaptations sont alors nécessaires, puisque la version 7.3 a introduit des schémas. Vous trouverez des informations complémentaires à l'adresse : http://www.ca.postgresql.org/docs/momjian/upgrade_tips_7.3.
- La version 4 de stunnel ne gère plus aucune option en ligne de commande. Le script /usr/sbin/stunnel3_wrapper qui est en mesure de convertir les options de ligne de commande dans un fichier de configuration approprié pour stunnel est néanmoins fourni et doit être utilisé à la demande (à la place d'OPTIONS, utilisez les vôtres) :

  ```
  /usr/sbin/stunnel3_wrapper stunnel OPTIONS
  ```

  Le fichier de configuration produit est aussi affiché sur la sortie par défaut, de sorte que vous pouvez utiliser aisément ces indications pour générer un fichier de configuration permanent pour l'avenir.
- openjade (openjade) est maintenant l'engin DSSSL qui remplace jade (jade_dsl) lorsqu'on appelle db2x.sh (docbook-toys). Pour des raisons de compatibilité, les divers programmes sont également mis à disposition sans le préfixe o.
  Si des applications particulières dépendent du répertoire jade_dsl et des fichiers qui y sont actuellement installés, il faut soit reconfigurer les applications en question pour prendre en compte le nouveau répertoire /usr/share/sgml/openjade, soit créer un lien en tant que root avec :

  ```
  cd /usr/share/sgml rm jade_dsl ln -s openjade jade_dsl
  ```

  Pour éviter un conflit avec le rzsz, l'outil en ligne de commande sx continue à être appellé s2x, sgml2xml ou osx.

4.2.2 De la version 8.2 à la version 9.0

Problèmes et particularités : `http://sdb.suse.com/sdb/en/2003/07/bugs90.html`.

- Le gestionnaire de paquetages RPM est actuellement disponible en version 4. La fonctionnalité prévue pour la compilation des paquetages est désormais transférée dans le programme autonome `rpmbuild`. `rpm` doit toujours être utilisé pour installer, mettre à jour et interroger la base de données. Voyez la section 4.3 page 137.
- Le paquetage `footmatic-filters` est maintenant disponible pour l'impression. Son contenu a été séparé du paquetage `cups-drivers` car il est apparu qu'on peut imprimer avec, même si CUPS n'est pas installé. On peut donc ainsi prendre en charge avec YaST des configurations qui sont indépendantes du système d'impression (CUPS, LPRng). Le fichier de configuration pour ce paquetage est `/etc/foomatic/filter.conf`.
- Désormais, les paquetages `footmatic-filters` et `cups-drivers` sont également requis pour la mise en œuvre des programmes LPRng et lpdfilter.
- Les ressources XML des paquetages logiciels fournis sont rendus accessibles grâce à des déclarations contenues dans `/etc/xml/suse-catalog.xml`. Ce fichier ne doit pas être traité avec `xmlcatalog` car sinon, des commentaires d'organisation nécessaires pour garantir une mise à jour en bonne et due forme disparaissent. `/etc/xml/suse-catalog.xml` est rendu accessible au moyen d'une instruction `nextCatalog`, de sorte que des outils XML comme `xmllint` ou `xsltproc` peuvent trouver automatiquement les ressources locales.

4.2.3 De la version 9.0 à la version 9.1

Consultez l'article "Problèmes et particularités de SUSE LINUX 9.1" dans la base de données support de SUSE sous `http://portal.suse.com` en le recherchant avec le mot-clé *particularités* ou *special features*. Ces articles sont publiés pour chaque version de SUSE LINUX.

Migration vers le noyau 2.6

SUSE LINUX a été complètement migrée vers le noyau version 2.6 ; vous ne devriez plus utiliser la version précédente 2.4, car les programmes ne fonctionneront pas. Vous trouverez ci-dessous quelques détails à prendre en compte :

- Le chargement des modules est configuré à partir du fichier `/etc/modprobe.conf` ; le fichier `/etc/modules.conf` est obsolète. YaST essaie de convertir le fichier (voir aussi le script `/sbin/generate-modprobe.conf`).

- Les modules ont désormais le suffixe `.ko`.
- Le module `ide-scsi` n'est plus nécessaire à la gravure des CD.
- Dans les options du module son ALSA, le préfixe `snd_` a été supprimé.
- `sysfs` complète désormais le système de fichiers `/proc`.
- La gestion de l'énergie (en particulier l'ACPI) a été améliorée et peut désormais être configurée avec un module de YaST.

Monter des partitions VFAT

Lors du montage de partitions VFAT, le paramètre `code=` doit être modifié en `codepage`. Si le montage d'une partition VFAT pose problème, vérifiez si le fichier `/etc/fstab` contient les anciens noms de paramètres.

Veille et attente (standby et suspend) avec ACPI

Avec le nouveau noyau 2.6 les modes veille et attente de ACPI sont supportés. Veuillez noter que ces fonctions en sont encore au stade expérimental et ne sont pas encore supportés par tous les matériels. Pour bénéficier de cette fonctionnalité, vous nécessitez le paquetage `powersave`. Vous trouverez plus d'informations relatives à ce paquetage sous `/usr/share/doc/packages/powersave`. Vous trouverez un frontal graphique dans le paquetage `kpowersave`.

Périphériques d'entrée

Concernant les changements relatifs aux périphériques d'entrée (input devices), reportez-vous à l'article susnommé du portail "Problèmes et particularités de SUSE LINUX 9.1" dans la base de données support de SUSE sous `http://portal.suse.com` en le recherchant avec le mot-clé *particularités* ou *special features*.

Native POSIX Thread Library et glibc 2.3.x

Les programmes liés à NGPT (*Next Generation POSIX Threading*) ne fonctionnent pas avec glibc 2.3.x. Tous les programmes de ce type qui ne font pas partie de la sélection d'applications accompagnant SUSE LINUX doivent être recompilés avec linuxthreads ou avec NPTL (*Native POSIX Thread Library*). Il est préférable d'utiliser NPTL pour le portage pour plus de pérennité vis-à-vis des standards futurs.

En cas de difficulté avec NPTL, il est possible d'utiliser linuxthreads, plus ancien, si la variable suivante est définie (dans laquelle ⟨*version-noyau*⟩ doit être remplacée par le numéro de version du noyau correspondant) :

```
LD_ASSUME_KERNEL=version-noyau
```

Les numéros de version suivants sont possibles :

2.2.5 (i386, i586) : linuxthreads sans piles flottantes (floating stacks)

2.4.1 (AMD64, i586, i686) : linuxthread avec piles flottantes

Remarque à propos du noyau et de linuxthreads avec piles flottantes : Les programmes qui utilisent `errno`, `h_errno` et `_res` doivent inclure les fichiers d'en-têtes correspondants (`errno.h`, `netdb.h` et `resolv.h`) avec `#include`. Les programmes C++ qui mettent en œuvre plusieurs fils d'exécution (multithread) et qui utilisent l'*annulation de fil d'exécution* (thread cancellation) doivent accéder à la variable d'environnement `LD_ASSUME_KERNEL=2.4.1` pour utiliser la bibliothèque linuxthreads.

Adaptations pour Native POSIX Thread Library

NPTL (*Native POSIX Thread Library*) est disponible dans SUSE LINUX 9.1 en tant que paquetage de gestion de fils de d'exécution. NPTL a été développé de manière à conserver une compatibilité binaire avec l'ancienne bibliothèque linuxthreads. Cependant, aux endroits auxquels linuxthreads enfreint la norme POSIX, NPTL a nécessité des adaptations. Il faut en particulier nommer : la gestion des signaux, `getpid` qui renvoie pour tous les fils d'exécution la même valeur, les gestionnaires de fils d'exécutions enregistrés avec pthread_atfork qui ne fonctionnent pas lorsque `vfork` est utilisé.

Configuration des interfaces réseau

La configuration des interfaces réseau a changé. Jusqu'à présent, l'initialisation du matériel était démarrée après la configuration d'une interface encore inexistante. Maintenant, le nouveau matériel sera tout d'abord recherché et initialisé à la suite de quoi l'interface réseau sera configurée.

De plus, de nouveaux noms ont été introduits pour les fichiers de configuration. Étant donné que le nom d'une interface réseau est générée dynamiquement et que le nombre de périphériques hotplug augmente sans arrêt, un nom tel que `eth0`, `eth1`, etc. n'est plus adapté à la configuration. Pour cette raison, nous

n'utilisons que des descriptions sans équivoque telles que l'adresse MAC ou le port PCI pour nommer les configurations des interfaces. Vous pouvez, bien entendu, utiliser les noms des interfaces dès qu'ils apparaissent. Des commandes telles que `ifup eth0` ou `ifdown eth0` sont toujours possibles.

Les configurations de périphériques se trouvent dans `/etc/sysconfig/hardware`. Les interfaces mises à disposition par ces périphériques se trouvent comme à l'habitude (avec des noms différents) dans `/etc/sysconfig/network`. Vous trouverez une description détaillée sous `/usr/share/doc/packages/sysconfig/README`.

Configuration du son

Après une mise à jour, les cartes son doivent être reconfigurées. Cela peut se faire à l'aide du module son de YaST. À cette fin, exécutez, en tant que `root`, la commande `yast2 sound`.

Domaine de premier niveau .local en tant que domaine link-local

La bibliothèque resolver traite le domaine de premier niveau `.local` en tant que domaine "link-local" et envoie des requêtes DNS multidiffusion à l'adresse de multidiffusion `224.0.0.251`, port `5353` au lieu de requêtes DNS normales. Ceci est une modification incompatible. Si le domaine `.local` est déjà utilisé dans la configuration du serveur de noms, il faut utiliser un autre nom de domaine. Vous trouverez plus d'informations au sujet de DNS multidiffusion sous `http://www.multicastdns.org`.

Encodage UTF-8 pour tout le système

`UTF-8` est désormais l'encodage par défaut du système. Lors d'une installation standard, une localisation avec l'indication d'encodage (encoding) `.UTF-8` est définie, comme par exemple, `fr_FR.UTF-8`. Vous trouverez plus d'informations sous `http://www.suse.de/~mfabian/suse-cjk/locales.html`.

Conversion UTF-8 des noms de fichiers

Les fichiers dans les systèmes de fichiers qui ont été créés auparavant n'utilisent pas d'encodage UTF-8 (tant que rien d'autre n'est précisé) pour les noms de fichiers. Si ces fichiers contiennent d'autres caractères que les caractères ASCII, ils apparaîtront "bizarrement". Pour éviter cela, le script `convmv` peut être utilisé ; il convertit l'encodage des noms de fichiers en UTF-8.

Outils Shell compatibles avec le standard POSIX de 2001

Les outils en mode interpréteur de commande (outils shell) provenant du paquetage `coreutils` (`tail`, `chown`, `head`, `sort`, etc.) ne suivent plus la norme POSIX de 1992 mais suivent dorénavant le réglage par défaut de la norme POSIX de 2001 (*Single UNIX Specification, version 3 == IEEE Std 1003.1-2001 == ISO/IEC 9945:2002*). Toutefois, l'ancien comportement peut être imposé à l'aide d'une variable d'environnement :

```
_POSIX2_VERSION=199209
```

La nouvelle valeur est 200112 et est acceptée comme norme pour `_POSIX2_VERSION`. Vous pouvez lire le standard SUS à l'adresse `http://www.unix.org` (gratuit, mais une inscription est nécessaire).

TAB. 4.1: *Comparatif POSIX 1992/POSIX 2001*

POSIX 1992	POSIX 2001
`chown tux.users`	`chown tux:users`
`tail +3`	`tail -n 3`
`head -1`	`head -n 1`
`sort +3`	`sort -k 4`
`nice -10`	`nice -n 10`
`split -10`	`split -l 10`

Astuce

Les logiciels provenant d'une tierce partie ne suivent probablement pas encore le nouveau standard ; dans ce cas il est conseillé de mettre la variable d'environnement comme décrit ci-dessus.

Astuce

/etc/gshadow obsolète

/etc/gshadow a été abandonné et supprimé car ses données sont superflues pour les raisons suivantes :

- glibc ne le prend pas en charge.
- Il n'existe pas d'interface officielle pour ce fichier, et il n'existe pas non plus d'interface dans la suite shadow.
- La plupart des outils qui vérifient les mots de passe de groupe ne s'appuient pas sur ce fichier et l'ignorent à cause des deux raisons précédemment énoncées.

OpenLDAP

Étant donné que le format des bases a changé, les bases de données doivent être générées à nouveau. Lors de la mise à jour, cette conversion est effectuée automatiquement. Cependant, dans certains cas particuliers, la conversion échouera.

La vérification de schéma a été considérablement améliorée. Ainsi, certaines opérations non conformes au standard mais possibles avec la version précédente du serveur LDAP ne sont maintenant plus possibles.

La syntaxe des fichiers de configuration a été partiellement modifiée par rapport aux ACL (listes de contrôle d'accès).

Après l'installation, vous trouverez plus d'informations relatives à la mise à jour dans le fichier /usr/share/doc/packages/openldap2/README.update

Apache 1.3 remplacé par Apache 2

Le serveur web Apache (version 1.3) a été remplacé par Apache 2. Une documentation détaillée pour la version 2.0 est disponible sur la page web http://httpd.apache.org/docs-2.0/en/.Une mise à jour d'un système avec installation d'un serveur HTTP effacera le paquetage Apache et installera Apache 2. Le système doit alors être adapté manuellement ou à l'aide de YaST. Les fichiers de configuration ne se trouvent plus maintenant sous /etc/httpd mais sous /etc/apache2.

Pour la façon de gérer simultanément plusieurs requêtes, on a le choix entre les fils d'exécution et les processus. Les processus sont gérés par un seul module appelé module de multi-traitement (multiprocessing module, MPM). Apache 2 utilise aussi un paquetage apache2-prefork (préféré pour la stabilité) ou apache2-worker. La réaction d'Apache 2 à ces requêtes est différente selon le MPM utilisé. Cela a principalement des conséquences sur les performances et sur

l'utilisation des modules. Ces points seront discutés plus en détails dans la section 30.4 page 547.

Apache 2 reconnaît maintenant le protocole Internet de l'avenir IPv6.

Il existe désormais un mécanisme grâce auquel les développeurs de module peuvent donner des indications sur l'ordre désiré de chargement des modules pour que l'utilisateur n'ait plus à s'en préoccuper. L'ordre dans lequel les modules sont démarrés est souvent important et était auparavant déterminé par l'ordre de chargement. Un module qui n'autorise l'accès qu'aux utilisateurs identifiés pour certaines ressources doit ainsi être appelé en premier afin que l'utilisateur qui n'a pas de droit d'accès ne puisse en aucun cas être amené à voir la page.

Les requêtes et réponses d'Apache peuvent passer à travers un filtre.

De samba~2.x à samba~3.x

Avec la mise à jour de samba~2.x par samba~3.x, l'authentification `winbind` n'est plus disponible. Les autres méthodes sont toujours possibles. Pour cette raison, les programmes suivants ont été supprimés :

```
/usr/sbin/wb_auth
/usr/sbin/wb_ntlmauth
/usr/sbin/wb_info_group.pl
```

Voir aussi : `http://www.squid-cache.org/Doc/FAQ/FAQ-23.html#ss23.5`.

Mise à jour de OpenSSH (version 3.8p1)

Le support `gssapi` a été remplacé par `gssapi-with-mic` afin d'éviter de possibles attaques MITM. Ces deux versions ne sont pas compatibles. Ceci signifie que vous ne pourrez pas vous authentifier avec des tiquets Kerberos depuis des distributions plus anciennes car d'autres méthodes d'authentification sont maintenant utilisées.

Applications SSH et terminal

Lors de l'accès depuis un ordinateur distant (surtout via SSH, telnet et RSH) entre une version 9 (dans la configuration par défaut, avec UTF-8 activé) et un système plus ancien (SUSE LINUX 9.0 et versions précédentes, produits pour lesquels UTF-8 n'étaient pas supportés ou activés par défaut), les applications de terminal peuvent afficher des caractères erronés.

Cela vient du fait que OpenSSH ne transmet pas de paramètres locaux et les paramètres par défaut des systèmes sont donc utilisés alors qu'ils ne correspondent peut-être pas avec les paramètres du terminal distant. Ceci concerne YaST en mode textuel ainsi que des applications qui sont exécutées depuis un ordinateur distant en tant qu'utilisateur normal (pas `root`). Les applications exécutées par `root` ne sont concernées que lorsque l'utilisateur a modifié les paramètres locaux pour `root` (uniquement `LC_CTYPE` est défini par défaut).

libiodbc a été rejeté

Les utilisateurs de FreeRADIUS doivent maintenant utiliser unixODBC car libiodbc a été rejeté.

Ressources XML dans /usr/share/xml

FHS (voir l'section A page 701) prévoit que les ressources XML (DTDs, feuilles de style, etc) soient installées dans `/usr/share/xml`. Pour cette raison, quelques répertoires ne se situent plus dans `/usr/share/sgml`. En cas de problème, vous devrez modifier les scripts ou makefiles qui y font référence ou utiliser les catalogues officiels (en particulier `/etc/xml/catalog` ou `/etc/sgml/catalog`).

Supports de données avec subfs

Les supports de données sont maintenant intégrés à l'aide de subfs. Maintenant, les supports de données amovibles ne doivent plus être montés manuellement à l'aide de `mount`. Il suffit de passer dans le répertoire de périphérique correspondant sous `/media` pour monter le dispositif. Les supports de données ne peuvent pas être démontés tant qu'un programme y accède.

4.2.4 De la version 9.1 à la version 9.2

Reportez vous à l'article "Known Problems and Special Features in SUSE LINUX 9.2" (en anglais) dans la base de données support à l'adresse `http://portal.suse.com`, en recherchant le mot clé *special features*.

Activer le pare-feu activé durant l'installation dans la boîte de dialogue de suggestions

SuSEFirewall2, la solution pare-feu fournie, est activée depuis la boîte de dialogue de suggestions vers la fin de l'installation pour accroître la sécurité. Cela

veut dire que tous les ports sont initialement fermés et qu'ils peuvent être ouverts, si nécessaire, dans la boîte de dialogue de suggestions Par défaut, vous ne pouvez pas vous connecter depuis des systèmes distants. Cela s'oppose à la navigation réseau ou aux applications multidiffusion telles que SLP, Samba ("voisinage réseau") et certains jeux. Vous pouvez ajuster les réglages du pare-feu à l'aide de YaST.

Si lors de l'installation ou la configuration d'un service, un accès au réseau est nécessaire, le module YaST correspondant ouvre les ports TCP et UDP utilisés sur toutes les interfaces internes et externes. Si cela n'est pas désiré, l'utilisateur peut fermer les ports dans le module YaST ou entreprendre une configuration détaillée du pare-feu.

TAB. 4.2: *Ports utilisés par des services importants*

Service	**Ports**
Serveur HTTP	Le pare-feu sera adapté grâce aux instructions "Listen" (uniquement pour TCP).
Courrier électronique (postfix)	smtp 25/TCP
Serveur Samba	netbios-ns 137/TCP; netbios-dgm 138/TCP; netbios-ssn 139/TCP; microsoft-ds 445/TCP
Serveur DHCP	bootpc 68/TCP
Serveur DNS	domain 53/TCP; domain 53/UDP
Serveur DNS	et prise en charge particulière du portmapper dans SuSEFirewall2
port mapper	sunrpc 111/TCP; sunrpc 111/UDP
Serveur NFS	nfs 2049/TCP
Serveur NFS	plus port mapper
Serveur NIS	active portmap
TFTP	tftp 69/TCP
CUPS (IPP)	ipp 631/TCP; ipp 631/UDP

KDE et prise en charge IPv6

Par défaut, la prise en charge IPv6 n'est pas activée pour KDE. Vous pouvez l'activer en utilisant l'éditeur `/etc/sysconfig` de YaST. La raison pour laquelle cette prise en charge n'est pas activée est que les adresses IPv6 ne sont pas supportées correctement par tous les fournisseurs d'accès Internet et que cela aboutirait donc à des messages d'erreur lors de la navigation sur le web et des délais dans l'affichage des pages web.

Mise à jour en ligne YaST et "paquetages delta"

YOU, le service de mise à jour en ligne de YaST supporte maintenant un type spécial de paquetage RPM qui ne contient que la différence binaire avec un paquetage donné. Cette technique réduit considérablement la taille des paquetages et la durée du téléchargement au dépend de la charge du processeur qui augmente pour assembler le paquetage final. Dans `/etc/sysconfig/onlineupdate`, spécifiez si YOU doit utiliser ces "paquetages delta". Consultez `file:///usr/share/doc/packages/deltarpm/README` pour les détails techniques.

Configuration du système d'impression

À la fin de l'installation (boîte de dialogue de suggestions), il faut veiller à ce que les ports utiles au système d'impression soient ouverts dans la configuration du pare-feu. Les ports 631/TCP et 631/UDP sont nécessaires à CUPS et ne devraient pas être bloqués pour un fonctionnement normal. Si on veut imprimer via LPD ou via SMB, le port 515/TCP (pour l'ancien protocole LPD) ou les ports utilisés par Samba doivent être accessibles.

Passage à X.Org

Le passage de XFree86 à X.Org est facilité par des liens de compatibilité pour que les fichiers et commandes importants puissent rester accessibles avec leurs anciens noms.

TAB. 4.3: *Commandes*

XFree86	X.Org
`XFree86`	`Xorg`
`xf86config`	`xorgconfig`
`xf86cfg`	`xorgcfg`

TAB. 4.4: *Fichiers journaux dans /var/log*

XFree86	X.Org
XFree86.0.log	Xorg.0.log
XFree86.0.log.old	Xorg.0.log.old

De plus, en raison du passage à X.org, le nom des paquetages est passé de XFree86* à xorg-x11*.

Émulateurs de terminal pour X11

Plusieurs émulateurs de terminal ont été supprimés car ils ne sont plus maintenus ou parce qu'ils ne fonctionnent pas dans l'environnement par défaut, en raison, spécialement, de leur absence de prise en charge de UTF-8. SUSE LINUX contient des terminaux tels que xterm, les terminaux KDE et GNOME et mlterm (Multilingual Terminal Emulator for X) qui peuvent remplacer aterm et eterm.

Modifications du paquetage powersave

Les fichiers de configuration /etc/sysconfig/powersave ont été modifiés :

TAB. 4.5: *Division des fichiers de configuration dans /etc/sysconfig/powersave*

Ancien	maintenant divisé en
/etc/sysconfig/powersave/common	common
	cpufreq
	events
	battery
	sleep
	thermal

/etc/powersave.conf n'existe plus et les variables existantes sont reprises dans les fichiers comme décrit dans le tableau 4.5 de la présente page. Si vous aviez procédé à des modifications des variables "event" de /etc/powersave.conf, celles-ci doivent être adaptées en conséquence dans /etc/sysconfig/powersave/events

Les dénominations des modes de veille (en anglais sleep states) ont été modifiées :

- suspend (ACPI S4, APM suspend)
- standby (ACPI S3, APM standby)

sont devenues :

- suspend to disk (ACPI S4, APM suspend)
- suspend to ram (ACPI S3, APM suspend)
- standby (ACPI S1, APM standby)

OpenOffice.org (OOo)

Répertoires : OOo est maintenant installé dans `/usr/lib/ooo-1.1` au lieu de `/opt/OpenOffice.org`. Le répertoire par défaut pour les paramètres des utilisateurs est maintenant `~/.ooo-1.1` au lieu de `~/OpenOffice.org1.1`.

Raccourcis : Il existe de nouveaux raccourcis pour le démarrage des composants d'OOo. Les correspondances sont décrites dans le tableau 4.6 de la présente page.

TAB. 4.6: *Raccourcis*

Ancien	Nouveau
/usr/X11R6/bin/OOo-calc	/usr/bin/oocalc
/usr/X11R6/bin/OOo-draw	/usr/bin/oodraw
/usr/X11R6/bin/OOo-impress	/usr/bin/ooimpress
/usr/X11R6/bin/OOo-math	/usr/bin/oomath
/usr/X11R6/bin/OOo-padmin	/usr/sbin/oopadmin
/usr/X11R6/bin/OOo-setup	–
/usr/X11R6/bin/OOo-template	/usr/bin/oofromtemplate
/usr/X11R6/bin/OOo-web	/usr/bin/ooweb
/usr/X11R6/bin/OOo-writer	/usr/bin/oowriter
/usr/X11R6/bin/OOo	/usr/bin/ooffice
/usr/X11R6/bin/OOo-wrapper	/usr/bin/ooo-wrapper

Les raccourcis prennent maintenant en charge l'option `--icons-set` pour basculer entre les jeux d'icônes KDE et GNOME. Les options suivantes ne sont plus prises en charge : `--default-configuration`, `--gui`, `--java-path`, `--skip-check`, `--lang` (les paramètres de langue (en anglais locales) déterminent maintenant la langue), `--messages-in-window` et `--quiet`.

Prise en charge de KDE et GNOME : Les extensions KDE et GNOME sont fournies séparément dans les paquetages `OpenOffice_org-kde` et `OpenOffice_org-gnome`.

Table de mixage kmix

La table de mixage kmix est installée par défaut. Pour le matériel haut de gamme, il existe des alternatives telles que les tables de mixages comme QAMix/KAMix, envy24control (uniquement ICE1712) ou hdspmixer (uniquement RME Hammerfall).

Graver des DVD

Par le passé, un patch appliqué au paquetage binaire de `cdrecord` permettait d'adapter le paquetage `cdrecord` afin de pouvoir graver des DVD. Maintenant, un nouveau paquetage binaire `cdrecord-dvd` contenant ce patch est installé.

Le programme `growisofs` du paquetage `dvd+rw-tools` peut maintenant graver tous les supports DVD (DVD+R, DVD-R, DVD+RW, DVD-RW, DVD+RL). Nous vous conseillons d'utiliser ce programme plutôt que le patch `cdrecord-dvd`.

Noyaux multiples

Il est possible d'installer des noyaux multiples en parallèle. Cette caractéristique permet aux administrateurs de mettre le noyau à niveau en installant un nouveau noyau, vérifiant que ce nouveau noyau fonctionne comme prévu puis en désinstallant l'ancien noyau. Bien que YaST ne prenne pas encore en charge cette caractéristique, il est facile d'installer et de désinstaller des noyaux depuis l'interpréteur de commandes en utilisant `rpm -i ⟨paquetage⟩.rpm`. Vous trouverez plus d'informations quant à la gestion des paquetages depuis la ligne de commande dans la section 4.3 page 137.

Le menu du chargeur d'amorçage par défaut contient une entrée noyau. Avant d'installer des noyaux multiple, il est utile d'ajouter une entrée pour les noyaux

supplémentaires afin qu'ils puissent être facilement sélectionnés. Le noyau qui était actif avant l'installation d'un nouveau noyau peut être accédé en tant que `vmlinuz.previous` et `initrd.previous`. En créant, dans le chargeur d'amorçage, une entrée similaire à l'entrée par défaut, et en la faisant correspondre à `vmlinuz.previous` et `initrd.previous` au lieu de `vmlinuz` et `initrd`, on peut accéder au noyau précédemment actif. De la même façon, GRUB et LILO prennent en charge les entrées joker. Consultez les pages d'info de GRUB (`info grub`) et les pages de manuel de `lilo.conf` (5) pour plus de détails.

4.2.5 De la version 9.2 à la version 9.3

Reportez vous à l'article "Known Problems and Special Features in SUSE LINUX 9.3" (en anglais) dans la base de données support de SUSE à l'adresse `http://portal.suse.com`, en recherchant le mot clé *special features*.

Démarrer l'installation manuelle à l'invite du noyau

Le mode d''installation manuelle' n'apparaît plus sur l'écran du chargeur d'amorçage. Vous pouvez toujours avoir linuxrc en mode manuel en utilisant `manual=1` à l'invite d'amorçage. Normalement, cela n'est pas nécessaire car vous pouvez définir les options d'installation directement à l'invite du noyau comme `textmode=1` ou un URL comme source d'installation.

Kerberos pour l'authentification réseau

`Kerberos` est le système d'authentification réseau par défaut au lieu de `heimdal`. Il n'est pas possible de procéder à la conversion d'une configuration heimdal existante automatiquement. Lors d'une mise à jour du système, des copies de sauvegarde des fichiers de configuration seront créées comme décrit dans le tableau 4.7 de la présente page.

TAB. 4.7: *Fichiers de sauvegarde*

Ancien fichier	Fichier de sauvegarde
/etc/krb5.conf	/etc/krb5.conf.heimdal
/etc/krb5.keytab	/etc/krb5.keytab.heimdal

La configuration du client (`/etc/krb5.conf`) est très semblable à celle de heimdal. Si rien de spécial n'a été configuré, il suffit de remplacer le paramètre `kpasswd_server` par `admin_server`

Il n'est pas possible de reprendre les données liées au serveur (kdc/kadmind). Après la mise à jour du système, l'ancienne base de données heimdal est toujours disponible sous `/var/heimdal` ; MIT kerberos maintient la base de donnée sous `/var/lib/kerberos/krb5kdc`.

Fichier de configuration X.Org

L'outil de configuration SaX2 écrit les paramètres de configuration de X.Org dans `/etc/X11/xorg.conf`. Lors d'une nouvelle installation, aucun lien de compatibilité de `XF86Config` vers `xorg.conf` n'est créé.

Configuration PAM

`common-auth` configuration PAM par défaut pour la section auth

`common-account` configuration PAM par défaut pour la section account

`common-password` configuration PAM par défaut pour la section password

`common-session` configuration PAM par défaut pour la gestion des sessions

Vous devriez inclure ces fichiers de configuration par défaut dans le fichier de configuration spécifique à votre application car il est plus facile de modifier et de maintenir un fichier de configuration plutôt qu'une quarantaine de fichiers qui existaient sur le système. Si vous installez une application plus tard, elle héritera des changements déjà appliqués et l'administrateur n'aura pas à penser à ajuster la configuration.

Les changements sont simples : si vous avez le fichier de configuration suivant (ce qui doit être le cas par défaut pour la plupart des applications) :

```
#%PAM-1.0
auth     required       pam_unix2.so
account  required       pam_unix2.so
password required       pam_pwcheck.so
password required       pam_unix2.so    use_first_pass use_authtok
#password required      pam_make.so     /var/yp
session required        pam_unix2.so
```

vous pouvez le changer en :

```
#%PAM-1.0
auth     include        common-auth
account  include        common-account
password include        common-password
session  include        common-session
```

4.3 RPM – Le gestionnaire de paquetages

Sous SUSE LINUX,le gestionnaire de paquetages RPM (RPM Package Manager) est chargé d'assurer la gestion des paquetages logiciels et s'appuie principalement sur les programmes `rpm` et `rpmbuild`. Ainsi, les utilisateurs et les administrateurs, sans oublier les créateurs de paquetages ont accès à toute la puissance de la base de données RPM, qu'ils peuvent interroger sans limites afin d'obtenir toutes les informations utiles sur les logiciels installés.

La commande `rpm` fonctionne essentiellement selon cinq modes : l'installation, la désinstallation ou la mise à jour de paquetages logiciels ; la régénération de la base de données RPM ; l'interrogation de la base de données RPM ou d'archives RPM données ; le contrôle d'intégrité des paquetages ; enfin la signature des paquetages. La commande `rpmbuild` est quant-à-elle chargée de générer les paquetages pouvant être installés à partir des sources originelles (pristine sources).

Les archives RPM pouvant être installées sont empaquetées dans un format binaire particulier ; elles comprennent les fichiers de programmes à installer ainsi que différentes méta-informations utilisées lors de l'installation par la commande `rpm` afin de configurer le paquetage logiciel concerné. Ces méta-informations sont également enregistrées dans la bases de données RPM dans une optique documentaire. Les archives RPM utilisent l'extension de fichier `.rpm`.

La commande `rpm` permet de gérer des paquetages conformes au standard LSB. Pour plus de précisions sur LSB, consultez l'section A page 701.

Astuce

Un nombre considérables de paquetages ont besoin de composants (bibliothèques, fichiers d'en-tête à inclure, etc.) indispensables pour le développement logiciel, et constitués en paquetages indépendants. Ces paquetages de développement sont uniquement requis par les utilisateurs désirant compiler eux-mêmes des logiciels, par exemple les nouveaux paquetages GNOME. Ces paquetages se reconnaissent généralement à leur extension `-devel`, pa exemple : `alsa-devel`, `gimp-devel`, et `kdelibs-devel`.

Astuce

4.3.1 Vérification de l'authenticité d'un paquetage.

Les paquetages RPM de SUSE LINUX sont signés à l'aide de GnuPG. La clé, fingerprint compris, est :

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F  9994 A84E DAE8 9C80 0ACA
```

La commande `rpm --checksig apache-1.3.12.rpm` permet de vérifier la signature d'un paquetage RPM, ce qui permet de s'assurer qu'il provient réellement de SUSE ou d'une autre source de confiance. Cette mesure de précaution est recommandée tout particulièrement avec les paquetages de mise à jour obtenus sur Internet. Notre clé de signature de paquetage est déposée par défaut dans `/root/.gnupg/`. Cette clé est également enregistrée dans le répertoire `/usr/lib/rpm/gnupg/`, afin de permettre aux utilisateurs normaux de vérifier par eux-même la signature des paquetages RPM.

4.3.2 Gestion des paquetages : installation, mise à jour et désinstallation

En temps normal, l'opération d'installation d'une archive RPM est simple : `rpm -i ⟨paquetage⟩.rpm`. Toutefois, cette commande par défaut installe un paquetage uniquement si les dépendances sont satisfaites et s'il n'y a pas de conflit. La commande `rpm` affiche, le cas échéant, un message d'erreur indiquant les paquetages requis pour satisfaire les dépendances. De son côté, la base de données s'assure de l'absence de conflit : en règle générale, un fichier ne peut être rattaché qu'à un seul paquetage. Il est possible de contourner cette règle en faisant appel à différentes options pour forcer `rpm` à ignorer ces paramètres par défaut. Cette faculté doit toutefois être réservée aux utilisateurs avertis, en raison des conséquences qu'il peut y avoir pour les mises à jour ultérieures du système.

Les options `-U` ou `--upgrade` et `-F` ou `--freshen` sont également intéressantes pour actualiser un paquetage, par exemple : `rpm -F ⟨paquetage⟩.rpm`. Cette opération supprime une éventuelle version antérieure du paquetage et installe la nouvelle version. La différence entre les deux versions est que l'option `-U` installe également les paquetages qui, jusqu'alors, n'étaient pas disponibles sur le système. Au contraire, l'option `-F` ne remplace un paquetage que s'il avait déjà été installé dans la version antérieure. Dans le même temps, la commande `rpm` essaye d'être respectueuse des *fichiers de configuration*, en utilisant la stratégie suivante :

- Dans le cas où un fichier de configuration n'a pas été modifié par l'administrateur système, la commande `rpm` installe la nouvelle version du fichier correspondant. L'administrateur n'a pas à intervenir.
- Lorsqu'un fichier de configuration a été modifié par l'administrateur, n'importe quand avant la mise à jour, la commande `rpm` sauvegarde dans ce cas le fichier avec l'extension `.rpmorig` ou `.rpmsave` (fichier de sauvegarde) et installe la nouvelle version à partir du paquetage RPM, dans le cas où une modification serait intervenue entre le fichier initial et le fichier provenant du paquetage de la mise à jour. Il est alors probable que vous soyez obligé d'ajuster le fichier qui vient d'être installé à l'aide de la copie de sauvegarde (`.rpmorig` ou `.rpmsave`), en fonctions de vos paramètres système. Assurez-vous ensuite d'effacer tous les fichiers `.rpmorig` et `.rpmsave` pour éviter des problèmes lors de mises à jour ultérieures.
- Les fichiers `.rpmnew` sont créés chaque fois qu'il existe déjà un fichier de configuration *et* et que l'option `noreplace` a été définie dans le fichier `.spec`.

Lorsqu'une mise à jour a été effectuée, tous les fichiers `.rpmorig`, `.rpmsave` et `.rpmnew` doivent être effacés après avoir été comparés, de manière à éviter tout conflit lors des mises à jour ultérieures. L'extension `.rpmorig` est choisie dans le cas où le fichier était inconnu de la base de données RPM.

Dans le cas contraire, c'est l'extension `.rpmsave` qui est utilisée. En d'autres termes, l'extension `.rpmorig` est utilisée pour les mises à jour d'un format tiers vers le format RPM et l'extension `.rpmsave` pour les mises à jour d'un ancien RPM en un nouveau RPM. Dans le cas de l'extension `.rpmnew`, il n'est pas possible de déterminer si l'administrateur système a modifié le fichier de configuration ou non. Vous trouverez une liste de ces fichiers dans `/var/adm/rpmconfigcheck`. Gardez à l'esprit que certains fichiers de configuration (par exemple `/etc/httpd/httpd.conf`) sont intentionnellement laissés inchangés afin de vous permettre de continuer à travailler avec vos propres paramètres.

L'option `-U` *n'est pas* un équivalent de la séquence désinstallation, avec l'option `-e` et installation avec l'option `-i`. Chaque fois que cela est possible, il est préférable de privilégier l'option `-U`.

Pour supprimer un paquetage, saisissez `rpm -e ⟨paquetage⟩`. Toutefois, la commande `rpm` ne supprime un paquetage que s'il ne subsiste plus de dépendances. Ainsi, il est théoriquement impossible de supprimer Tcl/Tk tant qu'un autre programme en a besoin. C'est d'ailleurs le rôle de la base de données RPM de veiller sur ces dépendances. Dans le cas exceptionnel où une opération de suppression s'avérerait impossible, malgré l'*absence* de dépendances, il peut être utile de reconstruire la base de données RPM à l'aide de l'option `--rebuilddb`.

4.3.3 RPM et correctifs

Afin d'assurer la sécurité de fonctionnement d'un système, il est indispensable d'intégrer régulièrement des paquetages de mise à jour dans le système afin de le mettre à jour. Jusqu'à présent, il n'était possible de corriger des bogues présents dans un paquetage qu'en remplaçant ce dernier intégralement. Lorsque l'on a affaire à des paquetages volumineux comportant des bogues dans de petits fichiers, le volume de données en cause peut devenir rapidement considérable. Cependant, SUSE propose une fonctionnalité dans RPM, permettant d'appliquer des correctifs à des paquetages.

L'exemple de pine illustre les considérations les plus intéressantes :

Le RPM correctif convient-il à mon système ?

Pour vous en assurer, vous devez dans un premier temps demander quelle est la version du paquetage. Dans le cas de l'application pine, la commande est la suivante :

```
rpm -q pine
pine-4.44-188
```

L'opération suivante consiste à examiner le correctif afin de déterminer s'il correspond précisément à cette version de pine :

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

Ce correctif correspond à trois versions différentes de pine. La version installée dans notre cas s'y trouve également, ce qui permet d'appliquer le correctif.

Quels sont les fichiers remplacés par le correctif ?

Il est facile, à partir du RPM correctif, d'identifier les fichiers affectés par le correctif en question. Le paramètre `-P` de `rpm` sert à sélectionner des fonctions propres aux correctifs. Ainsi, la liste des fichiers est obtenue à l'aide la commande suivante :

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

ou, dans le cas où le correctif est déjà installé, avec

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

Comment installer un correctif RPM dans le système ?
Les correctifs RPM sont utilisés de la même manière que les RPM normaux. La seule différence est que cela implique qu'un RPM approprié ait déjà été installé.

Quels sont les correctifs qui ont déjà été installés dans le système et pour quelles versions de paquetage ?
Il est possible d'afficher une liste de tous les correctifs ayant été installés dans le système en exécutant la commande `rpm -qPa`. La commande se présente alors comme suit si, comme c'est le cas dans notre exemple, nous avons un système auquel un correctif a déjà été appliqué :

```
rpm -qPa
pine-4.44-224
```

Dans le cas où vous souhaiteriez savoir, après quelque temps, quelle version de paquetage a été mise en place dans un premier temps, cette information se trouve également dans la base de données RPM. Ainsi, pour `pine`, cette information est obtenue à l'aide de la commande :

```
rpm -q --basedon pine
pine = 4.44-188
```

Pour de plus amples informations, notamment sur la fonctionnalité des correctifs de RPM, reportez-vous aux pages de manuel de `rpm` et `rpmbuild`.

4.3.4 Paquetages RPM delta

Les paquetages "RPM delta" contiennent la différence (c'est à dire le "delta") entre une ancienne version et une nouvelle version d'un paquetage RPM. Appliquer un RPM delta sur un ancien RPM résulte en un RPM nouveau complet ; il n'est même pas nécessaire d'avoir un copie de l'ancien RPM, un RPM delta peut également fonctionner avec le RPM installé. Les paquetages deltarpm sont même plus petits que les RPM correctifs ce qui peut représenter un avantage si vous

souhaitez transférer des paquetages de mise à jour sur Internet. L'inconvénient est qu'une mise à jour où des RPM delta sont impliqués nécessitent considérablement plus de cycles CPU qu'une mise à jour avec des RPM complets ou des correctifs. Pour que YaST utilise des paquetages RPM delta lors des sessions YOU, attribuez, dans `/etc/sysconfig/onlineupdate`, la valeur "yes" à `YOU_USE_DELTAS`.

Les binaires `prepdeltarpm`, `writedeltarpm`, et `applydeltarpm` font partie de la suite deltarpm et vous aide lors de la création et de l'application des paquetages RPM delta. Avec les commandes suivantes, vous pouvez créer un RPM delta appelé `new.delta.rpm` (si `old.rpm` et `new.rpm` sont présents):

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio

xdelta delta -0 old.cpio new.cpio delta

writedeltarpm new.rpm delta info new.delta.rpm
rm old.cpio new.cpio delta
```

En utilisant `applydeltarpm`, vous pouvez reconstruire le nouveau RPM, soit à partir du système de fichiers si l'ancien paquetage est déjà installé :

```
applydeltarpm new.delta.rpm new.rpm
```

soit en utilisant l'option `-r` si vous souhaitez le dériver de l'ancien RPM sans accéder au système de fichiers :

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

Consultez `file:///usr/share/doc/packages/deltarpm/README` pour des détails techniques.

4.3.5 Requêtes RPM

L'option `-q` (query) permet de demander des informations. Ceci vous permet d'examiner vous-même une archive RPM (en ajoutant l'option `-p`) et également d'interroger la base de données RPM des paquetages installés. Vous pouvez, par ailleurs, définir le type des informations à afficher à l'aide d'options supplémentaires. Voir le tableau 4.8 page suivante.

TAB. 4.8: *Les principales options de requêtes RPM*

`-i`	Informations relatives à un paquetage
`-l`	Liste de fichiers du paquetage
`-f FICHIER`	Demande le paquetage qui posséde le fichier ⟨*FICHIER*⟩ (le chemin complet doit être spécifié avec ⟨*FICHIER*⟩)
`-s`	Affichage de l'état des fichiers (implique `-l`)
`-d`	Affiche uniquement les fichiers de documentation (implique `-l`)
`-c`	Affiche uniquement les fichiers de configuration (implique `-l`)
`--dump`	Affiche toutes les informations (à utiliser avec `-l`, `-c`, ou `-d`)
`--provides`	Affiche les fonctionnalités du paquetage qui peuvent être demandées par un autre paquetage à l'aide du paramètre `--requires`
`--requires`, `-R`	Affiche les dépendances du paquetage
`--scripts`	Affiche les scripts d'installation (preinstall, postinstall, uninstall)

Par exemple, la commande `rpm -q -i wget` affiche l'information vue dans l'exemple 4.2 de la présente page.

Example 4.2: *rpm -q -i wget*

```
Name        : wget                         Relocations: (not relocatable)
Version     : 1.9.1                             Vendor: SUSE LINUX AG, Nuernberg, Germany
Release     : 50                            Build Date: Sat 02 Oct 2004 03:49:13 AM CEST
Install date: Mon 11 Oct 2004 10:24:56 AM CEST      Build Host: f53.suse.de
Group       : Productivity/Networking/Web/Utilities   Source RPM: wget-1.9.1-50.src.rpm
Size        : 1637514                          License: GPL
Signature   : DSA/SHA1, Sat 02 Oct 2004 03:59:56 AM CEST, Key ID a84edae89c800aca
Packager    : http://www.suse.de/feedback
URL         : http://wget.sunsite.dk/
Summary     : A tool for mirroring FTP and HTTP servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

L'option `-f` fonctionne uniquement si le nom complet, incluant le chemin, est connu. Indiquez autant de noms de fichiers que vous le voulez. Par exemple, la commande :

```
rpm -q -f /bin/rpm /usr/bin/wget
```

donne le résultat suivant :

```
rpm-4.1.1-191
wget-1.9.1-50
```

Dans le cas où une partie seulement du nom du fichier est connue, il faut utiliser un script shell comme dans l'exemple 4.3 de la présente page. Le nom partiel du fichier cherché doit être transmis en paramètre lors de l'appel du script.

Example 4.3: *Script de recherche de paquetages*

```
#! /bin/sh
for i in $(rpm -q -a -l | grep  $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```

La commande `rpm -q --changelog rpm` permet d'afficher précisément les informations (de mise à jour, de configuration, de modification, etc.) correspondant à un paquetage donné. Cet exemple montre les informations relatives au paquetage `rpm`. Toutefois, la base de données RPM n'affiche que les cinq derniers éléments. Toutes les entrées (des deux dernières années) sont contenues dans le paquetage lui-même. Cette requête ne fonctionne que lorsque le CD 1 est monté sous `/media/cdrom` :

```
rpm -qp --changelog /media/cdrom/suse/i586/rpm-4*.rpm
```

La base de données installée permet également de procéder à des vérifications. Ces opérations sont effectuées avec l'option `-V`, l'option `-y` ou l'option `--verify`. Ainsi, la commande `rpm` affiche tous les fichiers d'un paquetage qui ont été modifiés depuis l'installation. La commande `rpm` peut être complétée par des paramètres (jusqu'à huit) faisant référence aux modifications suivantes :

Tab. 4.9: *Options de vérification RPM*

`5`	Somme de contrôle MD5
`S`	Taille du fichier
`L`	Lien symbolique
`T`	Date/heure de modification
`D`	Numéros de périphérique (device numbers) majeur et mineur
`U`	Utilisateur (user)
`G`	Groupe (group)
`M`	Mode (droits et le type de fichier)

Un `c` s'affiche en plus dans le cas des fichiers de configuration. L'exemple suivant illustre des modifications du fichier `/etc/wgetrc` (de `wget`) :

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Les fichiers de la base de données RPM se trouvent dans `/var/lib/rpm`. Avec une partition `/usr` de 1 Go, la base de données peut très bien occuper 30 Mo d'espace disque ; ceci est particulièrement vrai après une mise à jour complète. Dans l'éventualité où la base de données semblerait excessivement volumineuse, la solution la plus efficace consiste à utiliser l'option `--rebuilddb` pour créer une nouvelle base de données s'appuyant sur la base de données existante. Il est recommandé de réaliser une sauvegarde de la base de données existante avant de la reconstituer. Par ailleurs, le script `cron` `cron.daily` crée des copies quotidiennes de la base de données (comprimées avec gzip) dans `/var/adm/backup/rpmdb`. Leur nombre est fixé par la variable `MAX_RPMDB_BACKUPS` (option par défaut : `5`) dans `/etc/sysconfig/backup`. La taille de chaque sauvegarde est en moyenne de 3 Mo pour un répertoire `/usr` de 1 Go.

4.3.6 Installation et compilation de paquetages sources

Tous les paquetages source de SUSE LINUX ont l'extension `.src.rpm` (source RPM).

Astuce

Ces paquetages peuvent être installés avec YaST, de la même manière que pour tout autre paquetage. Cependant, les paquetages source ne sont jamais marqués comme étant installés (`[i]`) dans le gestionnaire de paquetages, comme c'est le cas pour les autres paquetages. La raison en est que les paquetages source ne sont pas répertoriés dans la base de données RPM. Lorsque vous installez un paquetage source, seul le code source est ajouté au système. Le logiciel lui-même doit être compilé. Seules les applications *installées* sont répertoriées dans la base de données RPM.

Astuce

Les répertoires de travail de `rpm` et `rpmbuild` dans `/usr/src/packages` doivent exister (en l'absence de paramétrage personnalisé, tel qu'il peut être réalisé dans `/etc/rpmrc`) :

`SOURCES` pour les sources originales (fichiers `.tar.bz2` ou `.tar.gz`, etc.) ainsi que pour les adaptations propres à la distribution (généralement, fichiers `.diff` ou `.patch`).

`SPECS` pour les fichiers `.spec` chargés de contrôler la procédure de *build* à la manière d'une méta-makefile.

`BUILD` répertoire dans lequel les sources sont décompactées, un correctif leur est appliqué et elles sont compilées.

`RPMS` répertoire dans lequel les paquetages *binaires* sont enregistrés

`SRPMS` emplacement des RPM *source*

Lorsque vous installez un paquetage source avec YaST, les composants requis sont installés dans `/usr/src/packages` : les sources et les modifications qui y sont apportées dans `SOURCES` et le fichier `.spec` correspondant dans `SPECS`.

Avertissement

Évitez de faire des expériences avec des composants système importants (`glibc`, `rpm`, `sysvinit`, etc.), au risque de mettre en péril le fonctionnement de votre système.

Avertissement

Examinons à présent le paquetage `wget.src.rpm`. Après avoir installé le paquetage avec YaST, nous avons les fichiers :

```
/usr/src/packages/SOURCES/nops_doc.diff
/usr/src/packages/SOURCES/toplev_destdir.diff
/usr/src/packages/SOURCES/wget-1.9.1+ipvmisc.patch
/usr/src/packages/SOURCES/wget-1.9.1-brokentime.patch
/usr/src/packages/SOURCES/wget-1.9.1-passive_ftp.diff
/usr/src/packages/SOURCES/wget-LFS-20040909.tar.bz2
/usr/src/packages/SOURCES/wget-wrong_charset.patch
/usr/src/packages/SPECS/wget.spec
```

La commande `rpmbuild -b ⟨X⟩ /usr/src/packages/SPECS/wget.spec` lance la procédure de compilation. ⟨X⟩ est un joker pour différentes étapes du processus de build (voir l'affichage de l'option `--help` ou la documentation de RPM pour plus de détails). Nous nous contenterons ici de donner une explication succincte :

-bp Prépare les sources dans `/usr/src/packages/BUILD` : décompacte et applique les correctifs

-bc comme `-bp`, compilation en plus

-bi comme `-bc`, installation en plus. Attention, dans le cas où un paquetage ne prend pas en charge la fonctionnalité BuildRoot, des fichiers de configuration importants risquent d'être écrasés !

-bb comme `-bi`, avec, en outre, la création du paquetage binaire. En cas de succès de la compilation, ce fichier se trouve dans `/usr/src/packages/RPMS`.

-ba comme `-bb`, avec, en outre, la création du paquetage source. En cas de succès de la compilation, il est enregistré sous `/usr/src/packages/SRPMS`.

--short-circuit saute un certain nombre d'étapes.

Le RPM binaire créé peut finalement être installé à l'aide de la commande `rpm -i` ou, de préférence, à l'aide de la commande `rpm -U` . L'installation avec `rpm` le fait apparaître dans la base de données RPM.

4.3.7 Création de paquetages avec build

De nombreux paquetages présentent le risque de copier involontairement les fichiers dans le système en cours d'exécution. Pour éviter ce problème, vous pouvez utiliser `build` qui se charge de créer un environnement destiné à la compilation du paquetage. La mise en place de cet environnement où la racine du système est transplantée (chroot) suppose que l'on réserve une arborescence de paquetages complète pour le script `build`. Cette arborescence peut être créée sur

un disque dur, sur un système NFS ou sur DVD. Le script obtient l'emplacement correspondant à l'aide de la commande `build --rpms ⟨Chemin⟩`. Contrairement à la commande `rpm`, la commande `build` demande à ce que le fichier SPEC soit dans le même répertoire que les sources. Dans le cas où vous souhaitez recompiler wget, comme dans l'exemple précédent, et que le DVD est monté sur le système sous `/media/dvd`, exécutez les commandes suivantes en tant que `root` :

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

Un environnement minimal est ensuite mis en place dans `/var/tmp/build-root`. Le paquetage est construit dans cet environnement. Les paquetages ainsi créés sont ensuite enregistrés dans `/var/tmp/build-root/usr/src/packages/RPMS`

Le script `build` propose un certain nombre d'options supplémentaires. Ainsi, il est possible d'utiliser en priorité vos propres RPM, d'omettre l'initialisation de l'environnement de build ou de restreindre la commande `rpm` à l'un des niveaux précédemment décrits. La commande `build --help` et la page de manuel de `build` permettent d'obtenir de plus amples informations.

4.3.8 Outils pour les archives RPM et pour la base de données RPM

Midnight Commander (`mc`) peut afficher le contenu d'une archive RPM ou en copier des parties. Il représente ce genre d'archives à la manière d'un système de fichiers virtuel, toutes les commandes des menus de Midnight Commander étant disponibles. Les informations contenues dans les lignes d'en-tête tirées du fichier HEADER peuvent être affichées à l'aide de la touche F3. Les touches de direction et la touche Entrée permettent de naviguer dans l'arborescence de l'archive. Si nécessaire, la touche de fonction F5 permet de copier des composants.

KDE contient l'utilitaire kpackage qui est une interface pour `rpm`. Un module de YaST offre un gestionnaire de paquetages complet (voir la section 2.2.1 page 39).

Réparation du système

Outre de nombreux modules YaST pour l'installation et la configuration du système, SUSE LINUX offre également des fonctions de réparation du système installé. Ce chapitre décrit les différents types et niveaux de réparation du système. Le Système de Secours de SUSE peut vous donner accès aux partitions. Un administrateur système expérimenté peut l'utiliser pour réparer un système endommagé.

Étant donné qu'il n'est pas certain qu'un système endommagé pourra amorcer de lui-même et sachant qu'un système en fonctionnement est difficile à réparer, amorcez, pour une réparation, comme pour une nouvelle installation. Suivez les étapes décrites dans le chapitre 1 page 3 pour que le dialogue de sélection du mode d'installation s'ouvre. Sélectionnez alors l'option 'Réparation du système installé'.

Important

Sélection du support d'installation adéquat

Pour que le système de réparation fonctionne correctement, le support d'installation utilisé pour amorcer le système doit correspondre exactement au système installé.

Important

Sélectionnez ensuite comment la réparation du système doit être effectuée. Les possibilités dont vous disposez sont réparation automatique, réparation personnalisée et outils pour experts. Elles sont décrites dans ce chapitre.

5.1 Réparation automatique

Cette méthode est destinée à réparer un système endommagé dont la cause des dommages n'est pas connue. Une fois la sélection faite, il est procédé à une analyse détaillée du système installé. Étant donné le nombre de tests et vérifications à réaliser, cette analyse peut durer assez longtemps. Vous pourrez suivre la progression de cette procédure en bas de l'écran dans deux barres de progression. La barre supérieure affiche le déroulement du test en cours, la barre inférieure affichant quant à elle l'état global de l'analyse. Dans la fenêtre au-dessus, vous pouvez voir quel test est mené actuellement et quel en est le résultat. Voir la figure 5.1 page ci-contre. Les groupes de tests suivants sont exécutés lors de chaque analyse. Chaque groupe contient toute une série de vérifications individuelles.

Tables de partitions de tous les disques durs
La validité et la cohérence des tables de partitions de tous les disques durs détectés est vérifiée.

Partitions d'échange (swap) Les zones d'échange du système installé sont recherchées, vérifiées et éventuellement proposées pour être activées. Il est conseillé d'accepter l'activation afin d'augmenter la vitesse de réparation du système.

Systèmes de fichiers Pour chaque système de fichiers trouvé, une vérification spécifique est effectuée.

Entrées du fichier `/etc/fstab` L'intégrité et la cohérence des entrées du fichier sont vérifiées. Toutes les partitions valides sont montées.

Configuration du chargeur d'amorçage L'intégrité et la cohérence de la configuration du chargeur d'amorçage du système installé (GRUB ou LILO) sont vérifiées. Les périphériques boot et root sont testés et la disponibilité du module initrd est contrôlée.

Base de données de paquetages Ici, il est vérifié que tous les paquetages nécessaires à une installation minimale sont disponibles. Si vous le souhaitez, les paquetages de base peuvent aussi être analysés, cependant cela peut durer très longtemps en raison de leur nombre.

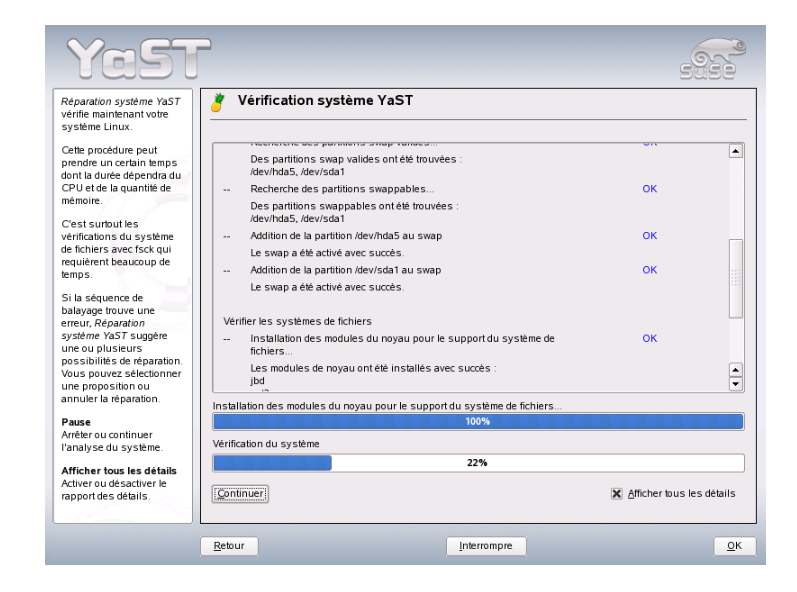


FIG. 5.1: *Mode de réparation automatique*

Lorsqu'une erreur est trouvée, l'analyse est arrêtée et une fenêtre de dialogue est ouverte. Cette fenêtre affiche des détails et propose des solutions. Étant donné le nombre de vérifications effectuées, il n'est pas possible de décrire ici tous les cas de figure. Veuillez lire les conseils affichés à l'écran, puis sélectionnez l'action

désirée. En cas de doute, vous pouvez également refuser la réparation proposée. Le système reste alors inchangé pour ce point. Aucune réparation n'est effectuée automatiquement sans demande de confirmation.

5.2 Réparation personnalisée

La réparation automatique décrite dans la section précédente procède à toutes les vérifications. Ceci n'est utile que lorsque l'origine des dommages du système est inconnue. Par contre, si vous savez quel zone du système est touchée, vous pouvez limiter ici le nombre des tests à effectuer. Après avoir sélectionné 'Réparation personnalisée', vous obtenez un choix de groupes de tests qui, dans un premier temps, sont tous sélectionnés. Dans ce cas, la vérification est la même que lors d'une réparation automatique. Si vous savez où l'erreur ne se situe pas, vous pouvez désélectionner les groupes correspondants. En cliquant sur 'Suivant', vous démarrez alors une procédure de test plus courte et donc plus rapide.

Notez cependant que les groupes de tests ne peuvent pas tous être appliqués seuls. La vérification des entrées fstab, par exemple, est toujours associée à la vérification du système de fichiers ainsi que des zones d'échange (swap) associées. YaST vérifie ces dépendances en sélectionnant automatiquement le nombre minimum de groupes de tests.

5.3 Outils pour experts

Si vous connaissez bien SUSE LINUX et que vous avez déjà une idée très concrète de ce qui doit être réparé dans votre système, vous pouvez, après avoir sélectionné 'Outils pour experts', utiliser les outils précis dont vous avez besoin pour la réparation.

Installer un nouveau chargeur d'amorçage
Ici, vous démarrez le module de configuration YaST du chargeur d'amorçage. Vous trouverez plus de détails à ce sujet dans la section 8.4 page 197

Démarrer le partitionneur Ici, vous démarrez le partitionneur YaST. Vous trouverez plus de détails à ce sujet dans la section 2.7.5 page 75.

Réparation du système de fichiers Vous pouvez vérifier ici les systèmes de fichiers de votre système installé. Vous disposez d'une sélection de toutes les partitions trouvées et vous pouvez y choisir celle que vous souhaitez vérifier.

Restaurer des partitions perdues Lorsque des tables de partitions de votre système sont endommagées, vous pouvez tenter ici une reconstruction. Une liste des disques durs détectés vous permet de choisir l'un d'entre eux. Cliquez sur 'OK' pour lancer la vérification. Cela peut prendre un certain temps, en fonction des performances de votre ordinateur et de la taille du disque dur.

Important

Reconstruction d'une table de partitions

La reconstruction d'une table de partitions est complexe. YaST essaie de reconnaître les partitions perdues à travers l'analyse des zones de données du disque dur. En cas de succès, les partitions retrouvées seront intégrées à la table de partitions reconstruite. Cependant, cela ne fonctionne pas à tous les coups.

Important

Enregistrer la configuration du système sur une disquette Avec cette option, vous pouvez enregistrer des fichiers importants du système sur une disquette. Si un de ces fichiers devait être endommagé plus tard, il pourrait être restauré à l'aide de la disquette.

Vérifier les logiciels installés Ici, la cohérence de la base de données de paquetages et la disponibilité des paquetages les plus importants sont vérifiées. Si des paquetages installés sont endommagés, vous pouvez ici requérir leur réinstallation.

5.4 Le système de secours SUSE

SUSE LINUX comporte un système de secours à l'aide duquel vous pouvez, en cas d'urgence, accéder de l'extérieur à vos partitions Linux : vous pouvez charger le système de secours (rescue system) à partir d'un CD, du réseau, ou du serveur FTP de SUSE. Le système de secours contient plusieurs programmes qui pourront vous aider à résoudre des problèmes de disques durs devenus inaccessibles, de fichiers de configuration erronés, etc.

Parted fait également partie du système de secours et est utilisé pour modifier les tailles des partitions. Il peut au besoin être lancé à partir du système de secours, si vous ne voulez pas utiliser le partitionneur intégré à YaST. Vous trouverez des informations sur Parted à l'adresse `http://www.gnu.org/software/parted/`.

5.4.1 Démarrer le système de secours

Amorcez votre système comme pour une installation. Sélectionnez 'Système de secours' depuis le menu d'amorçage. Le système de secours est alors décomprimé, chargé sur un disque RAM comme un nouveau système de fichiers racine, monté et démarré.

5.4.2 Utiliser le système de secours

Avec les combinaisons Alt-F1 jusqu'à Alt-F3, le système de secours met à votre disposition trois consoles virtuelles, sur lesquelles vous pouvez vous connecter comme utilisateur `root` sans mot de passe. Alt-F10 vous permet d'accéder à la console système affichant les messages du noyau et de syslog.

Vous trouverez dans le répertoire `/bin` l'interpréteur de commande et de nombreux autres utilitaires comme, par exemple, mount. Les utilitaires de fichiers et de réseau, par exemple pour contrôler et réparer des systèmes de fichiers comme reiserfsck, e2fsck, etc., se trouvent dans le répertoire `/sbin`. Dans ce répertoire, vous trouverez aussi les fichiers binaires les plus importants pour la maintenance du système comme fdisk, mkfs, mkswap, mount, init et shutdown et pour le fonctionnement du réseau comme ifconfig, route et netstat. Le répertoire `/usr/bin` contient l'éditeur vi, grep, find, less et telnet.

Accès au système normal

Le point de montage `/mnt` est destiné à monter votre système SUSE LINUX sur le disque lorsque vous utilisez le système de secours. Vous pouvez également créer d'autres répertoires et les utiliser comme points de montage. L'exemple suivant montre la procédure pour un système composé d'après `/etc/fstab` comme décrit dans exemple 5.1 de la présente page.

Example 5.1: */etc/fstab exemple*

```
/dev/sdb5       swap        swap        defaults   0   0
/dev/sdb3       /           ext2        defaults   1   1
/dev/sdb6       /usr        ext2        defaults   1   2
```

Avertissement

Considérez dans la section suivante l'ordre dans lequel les périphériques doivent être montés.

Avertissement

Afin d'avoir accès à tout le système, montez-le pas à pas sous `/mnt` avec les instructions suivantes :

```
mount /dev/sdb3 /mnt
mount /dev/sdb6 /mnt/usr
```

Vous avez désormais accès à tout le système et pouvez, par exemple, réparer les erreurs dans les fichiers de configuration comme `/etc/fstab`, `/etc/passwd` et `/etc/inittab`. Les fichiers de configuration ne se trouvent alors plus dans le répertoire `/etc` mais dans le répertoire `/mnt/etc`. Pour récupérer les partitions perdues en les recréant simplement avec le programme fdisk, imprimez `/etc/fstab` et le résultat de la commande `fdisk -l`.

Réparation des systèmes de fichiers

Des systèmes de fichiers endommagés sont une raison particulièrement valable de recourir au système de secours. Les systèmes de fichiers ne peuvent en principe pas être réparés quand le système est en marche. En cas de dommages importants, le système de fichiers racine ne peut le cas échéant même pas être monté et le démarrage du système se termine par un `kernel panic`. Il ne reste alors que la solution de tenter la réparation par l'extérieur à l'aide d'un système de secours.

Les utilitaires reiserfsck, e2fsck et dumpe2fs (pour le diagnostic) sont inclus dans le système de secours de SUSE LINUX. Vous pouvez résoudre ainsi la plupart des problèmes. Dans un tel cas d'urgence, les pages de manuel de reiserfsck et de e2fsck ne sont souvent plus accessibles, elles sont donc imprimées dans dans ce manuel dans section B page 703 et section B page 707.

Si un système de fichiers `ext2` ne peut plus être monté à cause d'un superbloc invalide, le programme e2fsck échouera sans doute aussi. La solution consiste à utiliser les sauvegardes de superblocs créées et maintenues à jour dans le système de fichiers tous les 8192 blocs (8193, 16385. . .). Pour cela, exécutez la commande `e2fsck -f -b 8193 /dev/damaged_partition`. L'option `-f` force la vérification du système de fichiers prévient ainsi l'erreur possible de `e2fsck` de façon à ce que tout fonctionne car le copie du superbloc est intact.

Deuxième partie

Système

Applications 32 bits et 64 bits dans un environnement système 64 bits

SUSE LINUX est disponible pour plusieurs plateformes 64 bits. Ceci ne signifie pas nécessairement que toutes les applications incluses dans la distribution ont déjà été adaptées pour les plateformes 64 bits. SUSE LINUX permet d'utiliser des applications 32 bits dans un environnement système 64 bits. Ce chapitre vous donne un petit aperçu de la façon dont cela se passe sur des plateformes SUSE LINUX 64 bits. Il explique comment sont exécutées les applications 32 bits (environnement d'exécution) et comment les applications 32 bits devraient être compilées pour leur permettre d'être exécutées à la fois dans un environnement système 32 bits et dans un environnement 64 bits. De plus, vous trouverez des informations sur l'interface de programmation du noyau ainsi que des explications pour exécuter des applications 32 bits avec un noyau 64 bits.

SUSE LINUX pour les plateformes 64 bits AMD64 et EM64T a été conçue de façon à ce que les applications 32 bits existantes soient utilisables "telles quelles" dans l'environnement 64 bits. Ainsi, il vous est possible de continuer à utiliser vos applications 32 bits favorites sans avoir à attendre qu'une adaptation 64 bits correspondante ne soit disponible.

6.1 Prise en charge de l'environnement d'exécution

Important

Conflits entre versions d'une même application

Si une application est disponible aussi bien pour 32 bits que pour 64 bits, une installation parallèle des deux versions posera inévitablement des problèmes. Dans de tels cas, vous devez vous décider pour l'une ou l'autre des deux versions, installer celle-ci et l'utiliser.

Important

Chaque application nécessite une série de bibliothèques pour être exécutée correctement. Les désignations pour les versions 32 bits et 64 bits de cette bibliothèque sont malheureusement identiques. Elles doivent se différencier l'une de l'autre d'une autre façon.

Pour maintenir la compatibilité avec la version 32 bits, les bibliothèques sont enregistrées dans le système au même emplacement que dans l'environnement 32 bits. La version 32 bits de `libc.so.6` se trouve dans `/lib/libc.so.6` aussi bien dans l'environnement 32 bits que dans l'environnement 64 bits.

Toutes les bibliothèques 64 bits et les fichiers objet se trouvent dans des répertoires appelés `lib64`. Ainsi, des fichiers objet 64 bits que vous chercheriez normalement dans `/lib`, `/usr/lib` et `/usr/X11R6/lib` se trouvent maintenant dans `/lib64`, `/usr/lib64` et `/usr/X11R6/lib64`. L'espace reste donc disponible pour les bibliothèques 32 bits dans `/lib`, `/usr/lib` et `/usr/X11R6/lib` et le nom de fichier peut être conservé entre les deux versions.

En principe, les sous-répertoires des répertoires objet dont le contenu des données est indépendant de la taille du mot, ne sont pas déplacés. Par exemple, vous trouverez toujours les polices X11 à l'emplacement habituel`/usr/X11R6/lib/X11/fonts`. Ce schéma est conforme à la LSB (>Linux Standards Base) et au FHS (File System Hierarchy Standard).

6.2 Développement de logiciels

Une chaîne de développement bi-architecture permet de générer aussi bien des objets 32 bits que des objets 64 bits. Le comportement par défaut est de compiler des objets 64 bits. On peut générer des objets 32 bits en utilisant des drapeaux spéciaux. Pour GCC, ce drapeau spécial est `-m32`.

Notez que tous les fichiers d'en-tête doivent être écrits dans une forme indépendante de l'architecture et que les bibliothèques installées 32 et 64 bits doivent présenter une API (interface de programmation d'applications) en accord avec les fichiers d'en-tête installés. L'environnement SUSE normal est conçu suivant ce principe. Pour les bibliothèques que vous mettez à jour vous-même, vous devez vous occuper personnellement de ces questions.

6.3 Compilation de logiciels sur des plateformes bi-architecture

Pour développer sur une bi-architecture des fichiers binaires pour l'autre architecture, vous devez en outre installer les bibliothèques correspondant à la seconde architecture. Ces paquetages s'appellent `nomrpm-32bit` . Vous avez aussi besoin des fichiers d'en-tête et des bibliothèques correspondants des paquetages `nomrpm-devel` et des bibliothèques de développement pour la seconde architecture que vous trouverez dans `nomrpm-devel-32bit` .

La plupart des programmes Open Source utilisent une procédure de configuration de programme basée sur `autoconf`. Pour utiliser `autoconf` pour la configuration d'un programme pour la seconde architecture, vous devez écraser les réglages normaux du compilateur et de l'éditeur de liens de `autoconf` en appelant les scripts `configure` avec des variables d'environnement supplémentaires.

L'exemple suivant se base sur un système AMD64 et EM64T avec x86 comme seconde architecture :

1. Configurez `autoconf` pour utiliser le compilateur 32-bits :

   ```
   CC="gcc -m32"
   ```

2. Donnez l'ordre à l'éditeur de liens de traiter les objets 32 bits :

   ```
   LD="ld -m elf64_i386"
   ```

3. Demandez à l'assembleur de créer des objets 32 bits :

   ```
   AS="gcc -c -m32"
   ```

4. Faites en sorte que `libtool` et autres outils aillent chercher les bibliothèques dans `/usr/lib` :

   ```
   LDFLAGS="-L/usr/lib"
   ```

5. Définissez l'emplacement des bibliothèques comme étant le sous-répertoire `lib` :

   ```
   --libdir=/usr/lib
   ```

6. Indiquez que les bibliothèques de X 32 bits sont utilisées :

   ```
   --x-libraries=/usr/X11R6/lib/
   ```

Ces variables ne sont pas toutes nécessaires pour chaque programme. Adaptez-les aux différents programmes.

```
CC="gcc -m64"            \
LDFLAGS="-L/usr/lib64;"  \
        .configure       \
          --prefix=/usr  \
          --libdir=/usr/lib64
make
make install
```

6.4 Spécifications du noyau

Les noyaux 64 bits pour AMD64 et EM64T proposent une interface binaire aux applications (ABI, Application Binary Interface) aussi bien 64 que 32 bits. Cette dernière est identique à l'ABI du noyau 32 bits correspondant. Ceci signifie que l'application 32 bits peut communiquer avec le noyau 64 bits de la même manière qu'avec le noyau 32 bits.

Veuillez noter que l'émulation 32 bits d'appels système d'un noyau 64 bits ne prend pas en charge un certain nombre d'API utilisées par les programmes système. Ceci dépend de la plateforme. Pour cette raison, un petit nombre d'applications comme `lspci` ou les programmes d'administration LVM doivent être compilées en tant que programmes 64 bits pour fonctionner correctement.

Un noyau 64 bits ne peut charger que des modules noyau 64 bits spécialement compilés pour ce noyau. Il n'est pas possible d'utiliser des modules noyau 32 bits.

Astuce

Quelques applications nécessitent leurs propres modules pouvant être chargés par le noyau. Si vous avez l'intention d'utiliser une telle application 32 bits dans un environnement système 64 bits, contactez le fournisseur de cette application et SUSE pour être sûr que la version 64 bits du module pouvant être chargé par le noyau et la version compilée en 32 bits des API du noyau sont disponibles pour ce module.

Astuce

Amorcer et configurer un système Linux

L’amorçage d’un système Linux est une procédure complexe. De nombreux composants différents sont impliqués et doivent interagir sans heurts. Ce chapitre fournit une description sommaire des principes sous-jacents et des composants qui interviennent. Le principe des niveaux d’exécution et la configuration du système SUSE avec `sysconfig` sont également abordés ci-après.

7.1 Le processus d’amorçage de Linux

Le processus d’amorçage de Linux se compose de plusieurs étapes dont chacune est représentée par un autre composant. La liste suivante résume brièvement le processus d’amorçage et décrit tous les composants majeurs concernés.

1. **Le BIOS**

   Une fois que l’ordinateur est allumé, le BIOS initialise l’écran et le clavier, puis teste la mémoire centrale. Jusqu’à ce stade, la machine n’accède à aucun support de stockage de masse.

   Par la suite, les informations sur la date et l’heure actuelles, ainsi que les périphériques sont chargés à partir des valeurs en mémoire non volatile (*Réglages CMOS*). Lorsque le premier disque dur et sa géométrie sont reconnus, le contrôle du système passe du BIOS au chargeur d’amorçage.

2. **Le chargeur d’amorçage**

   Le premier secteur de données physiques de 512 octets du premier disque dur est chargé dans la mémoire centrale et le *chargeur d’amorçage*, placé au début de ce secteur, prend le contrôle. Les commandes exécutées par le chargeur d’amorçage déterminent le reste du processus d’amorçage. Par conséquent, les 512 premiers octets du disque dur sont appelés *Master Boot Record* (MBR, secteur d’amorçage maître). Le chargeur d’amorçage passe ensuite le contrôle au système d’exploitation proprement dit, dans ce cas, le noyau Linux. Vous trouverez plus d’informations sur GRUB, le chargeur d’amorçage de Linux dans le chapitre 8 page 183.

3. **Le noyau et initrd**

   Pour transmettre le contrôle du système, le chargeur d’amorçage charge à la fois le noyau et un disque virtuel (RAM disk) initial en mémoire. Le noyau Linux offre la possibilité d’avoir de petits systèmes de fichiers chargés dans un disque virtuel et de lancer des programmes avant que le système de fichiers racine proprement dit ne soit monté. Le noyau décompresse ensuite l’initrd et le monte à titre de système de fichiers racine temporaire. Le contenu d’initrd est un système Linux minimal qui contient un exécutable appelé linuxrc. Cet exécutable est exécuté avant que le système de fichiers racine réel ne soit monté. Lorsque cela est possible, le noyau libère la mémoire occupée par initrd et démarre init dès que linuxrc a terminé sa tâche. Vous trouverez plus d’informations sur initrd dans la section 7.1.1 page suivante.

4. **linuxrc**

   Ce programme effectue toutes les actions nécessaires pour monter le véritable système de fichiers racine comme fournir les fonctionnalités du noyau pour le système de fichiers nécessaire et les pilotes de périphériques pour les contrôleurs de mémoire de masse. Dès que le système de fichiers réel a été monté avec succès, linuxrc s'arrête et le noyau démarre le programme init. Vous trouverez plus d'informations sur linuxrc dans la section 7.1.2 page suivante.

5. **init**

   init prend en charge l'amorçage effectif du système par l'intermédiaire de plusieurs niveaux différents qui fournissent différentes fonctionnalités. init est décrit dans la section 7.2 page 169.

7.1.1 initrd

initrd est un petit système de fichiers (généralement compressé) que le noyau peut charger dans un disque virtuel puis monter en tant que système de fichiers temporaire. Il fournit un environnement Linux minimal qui permet d'exécuter des programmes avant que le système de fichiers racine réel ne soit monté. Cet environnement Linux minimal est chargé en mémoire par les routines BIOS et ne nécessite pas une configuration matérielle particulière autre que suffisamment de mémoire. initrd doit toujours fournir un exécutable nommé linuxrc qui doit être quitté sans erreur.

Avant que le système de fichiers racine réel puisse être monté et le système d'exploitation réel ne soit démarré, le noyau a besoin des pilotes correspondants pour accéder au périphérique sur lequel réside le système de fichiers racine. Ces pilotes peuvent contenir des pilotes spéciaux pour un certain type de disques durs, voire des pilotes réseau pour accéder à un système de fichiers en réseau (voir page suivante). Le noyau doit également contenir le code nécessaire pour lire le système de fichiers de initrd. Les modules pour le système de fichiers racine peuvent être chargés par linuxrc.

Créez un `initrd` avec le script `mkinitrd`. Dans SUSE LINUX, les modules à charger sont indiqués par la variable `INITRD_MODULES` dans le fichier `/etc/sysconfig/kernel`. Après l'installation, cette variable se voit automatiquement affecter la valeur correcte (le linuxrc d'installation enregistre la liste des modules qui ont été chargés). Les modules sont chargés dans l'ordre exact dans lequel ils apparaissent dans `INITRD_MODULES`. C'est particulièrement important si

l'on fait appel à plusieurs pilotes SCSI, car sinon les noms des disques durs changeraient. À proprement parler, il serait suffisant de ne charger que ces pilotes nécessaires pour accéder au système de fichiers racine. Cependant, tous les pilotes SCSI requis pour l'installation sont chargés au moyen d'initrd car les charger plus tard pourrait être problématique.

Important

Mettre à jour initrd

Le chargeur d'amorçage charge initrd de la même manière que le noyau. Il n'est pas nécessaire de réinstaller GRUB après la mise à jour de l'initrd, car GRUB cherche dans le répertoire le fichier correct lors de l'amorçage.

Important

7.1.2 linuxrc

L'objectif principal de linuxrc est de préparer le montage du système de fichiers racine réel et l'accès à ce dernier. Selon votre configuration système effective, linuxrc se charge des tâches suivantes.

Charger les modules du noyau Selon votre configuration matérielle, des pilotes spéciaux peuvent être nécessaires pour accéder aux composants matériels de votre ordinateur (le composant le plus important étant votre disque dur). Pour accéder au système de fichiers racine final, le noyau doit charger les pilotes appropriés du système de fichiers.

Gérer les configurations RAID et LVM Si vous avez configuré votre système qui contienne le système de fichiers racine en RAID ou sous LVM, linuxrc configure LVM ou le RAID pour permettre d'accéder plus tard au système de fichiers racine. Vous trouverez plus d'informations sur le RAID dans la section 3.8 page 111. D'autres information sur LVM sont disponibles dans la section 3.7 page 104.

Gérer la configuration réseau Si vous avez configuré votre système pour utiliser un système de fichiers racine monté en réseau (monté via NFS), linuxrc doit être sûr que les pilotes réseau corrects sont chargés et qu'ils sont configurés pour permettre l'accès au système de fichiers racine.

Quand linuxrc est appelé au cours de l'amorçage initial en tant que partie de la procédure d'installation, ses tâches diffèrent de celles mentionnées plus haut :

Trouver le support d'installation Lorsque vous démarrez le processus d'installation, votre machine charge un noyau d'installation et un initrd spécial avec l'utilitaire d'installation YaST à partir du support d'installation. Le programme d'installation YaST, qui est exécuté dans un système de fichiers en mémoire vive, doit avoir des informations sur l'emplacement réel du support d'installation pour y accéder et installer le système d'exploitation.

Démarrer la reconnaissance du matériel et charger les modules de noyau appropriés
Comme mentionné dans la section 7.1.1 page 167, le processus d'amorçage démarre avec un ensemble minimal de pilotes que l'on peut utiliser avec la plupart des configurations matérielles. linuxrc démarre un processus initial d'analyse du matériel qui détermine l'ensemble de pilotes appropriés pour votre configuration matérielle. Ces valeurs sont écrites ultérieurement dans `INITRD_MODULES`, dans le fichier `/etc/sysconfig/kernel` pour permettre à n'importe quel processus d'amorçage qui viendrait plus tard d'utiliser un initrd personnalisé. Pendant le processus d'installation, linuxrc charge cet ensemble de modules.

Charger le système d'installation ou le système de secours
Dès que le matériel a été correctement reconnu et que les pilotes appropriés ont été chargés, linuxrc démarre le système d'installation qui contient le programme d'installation YaST réel ou le système de secours.

Démarrer YaST Pour finir, linuxrc démarre YaST, qui démarre à son tour l'installation des paquetages et la configuration du système.

7.1.3 Pour plus d'informations

Pour plus d'informations, voir `/usr/src/linux/Documentation/ramdisk.txt`, `/usr/src/linux/Documentation/initrd.txt`, ainsi que les pages de manuel initrd(4) et mkinitrd(8).

7.2 Le programme init

Le programme init est le processus portant le numéro de processus 1 et qui responsable d'initialiser le système proprement dit de la manière requise. Tous les autres processus sont des processus enfants d'init ou d'un de ses enfants. init joue un rôle particulier. Il est démarré directement par le noyau et résiste au signal 9,

qui normalement tue les processus. Tous les autres programmes sont démarrés soit directement par init, soit par un de ses processus enfants.

init est configuré de manière centralisée dans le fichier `/etc/inittab`, où sont définis les *niveaux d'exécution* (run levels) (voir la section 7.3 de la présente page). Il précise également quels sont les services et démons disponibles dans chacun des niveaux. En fonction des éléments contenus dans le fichier `/etc/inittab`, init exécute plusieurs scripts. Pour des raisons de clarté, ces scripts résident tous dans le répertoire `/etc/init.d`.

init maintient le processus entier de démarrage du système et de son arrêt. De ce point de vue, le noyau peut être considéré comme un processus d'arrière-plan dont la tâche est de maintenir tous les autres processus et d'ajuster le temps machine ainsi que l'accès au matériel en fonction des requêtes provenant d'autres programmes.

7.3 Les niveaux d'exécution

Sous Linux, les *niveaux d'exécution* définissent la manière dont le système est démarré et quels services sont disponibles dans le système en fonctionnement. Après l'amorçage, le système démarre comme défini dans le fichier `/etc/inittab`, dans la ligne `initdefault`. Il s'agit habituellement du niveau d'exécution `3` ou `5`. Voir le tableau 7.1 page suivante. Il est également possible d'indiquer le niveau d'exécution au moment de l'amorçage (à l'invite d'amorçage, par exemple). Tout paramètre qui n'a pas été directement évalué par le noyau lui-même est passé à init.

Pour changer de niveau d'exécution tandis que le système tourne, saisissez `init` et le nombre correspondant comme argument. Seul l'administrateur système est habilité à le faire. `init 1` (ou `shutdown now`) fait passer le système en *mode mono-utilisateur* qui est employé pour la maintenance et l'administration du système. Une fois son travail terminé, l'administrateur peut revenir au niveau d'exécution normal en saisissant `init 3`, qui démarre tous les programmes essentiels et permet aux utilisateurs normaux de se connecter, puis de travailler sur le système sans X. Pour activer un environnement graphique comme GNOME, KDE ou tout autre gestionnaire de fenêtres, utilisez `init 5` à la place. `init 0` ou `shutdown -h now` entraîne l'arrêt du système. `init 6` ou `shutdown -r now` le fait s'arrêter puis redémarrer.

Important

Niveau d'exécution 2 avec une partition /usr montée via NFS

Vous ne devriez pas utiliser le niveau d'exécution 2 si votre système monte la partition `/usr` via NFS. Le répertoire `/usr` contient des programmes importants essentiels pour le fonctionnement correct du système. Du fait que le service NFS n'est pas disponible dans le niveau d'exécution 2 (mode multi-utilisateur local sans réseau distant), le système serait fortement restreint par bien des aspects.

Important

TAB. 7.1: *Niveaux d'exécution disponibles*

Niveau d'exécution	Description
0	Arrêt du système
S	Mode mono-utilisateur ; à partir de l'invite d'amorçage, seulement avec une disposition du clavier américaine
1	Mode mono-utilisateur
2	Mode multi-utilisateur local sans réseau distant (par exemple NFS)
3	Mode multi-utilisateur complet avec réseau
4	Non utilisé
5	Mode multi-utilisateur complet avec réseau et gestionnaire d'affichage X—KDM (par défaut), GDM ou XDM
6	Redémarrage du système

Le niveau d'exécution 5 est le niveau d'exécution par défaut dans toutes les installations standard de SUSE LINUX. Les utilisateurs sont invités à se connecter directement sous une interface graphique. Si le niveau d'exécution par défaut est 3, le système X Window doit être configuré correctement, comme décrit dans le chapitre 11 page 233, avant que le niveau d'exécution ne passe à 5.S'il en est ainsi, vérifiez si le système fonctionne de la manière souhaitée en saisissant `init 5`. Si tout se déroule comme prévu, vous pouvez faire appel à YaST pour régler le niveau d'exécution par défaut à 5.

Avertissement

Modifier /etc/inittab

Si `/etc/inittab` est endommagé, le système pourrait ne pas amorcer correctement. Soyez donc extrêmement prudent lorsque vous modifiez `/etc/inittab` et conservez toujours une sauvegarde d'une version intacte. Pour réparer les dommages, essayez de saisir `init=/bin/sh` après le nom du noyau à l'invite d'amorçage pour amorcer directement dans un interpréteur de commandes. Ensuite, rendez votre système de fichiers inscriptible à l'aide de la commande `mount -o remount,rw /` et remplacez `/etc/inittab` par votre version de sauvegarde à l'aide de la commande `cp`. Pour éviter des erreurs du système de fichiers, repassez votre système de fichiers en lecture seule avant de réamorcer : `mount -o remount,ro /`.

Avertissement

7.4 Changer de niveau d'exécution

Généralement, deux événements se produisent quand vous changez de niveau d'exécution. Tout d'abord, les scripts d'arrêt du niveau d'exécution actuel sont lancés, ce qui ferme certains programmes essentiels pour le niveau d'exécution actuel. Ensuite, les scripts de démarrage du nouveau niveau d'exécution sont démarrés. Dans la plupart des cas, un certain nombre de programmes sont démarrés ici. Par exemple, voici ce qui se produit en passant du niveau d'exécution 3 au niveau 5.

1. L'administrateur (`root`) ordonne à init de passer à un niveau d'exécution différent en saisissant `init 5`.
2. init consulte son fichier de configuration (`/etc/inittab`) et décide qu'il devrait démarrer `/etc/init.d/rc` avec le nouveau niveau d'exécution comme paramètre.
3. À présent, `rc` appelle tous les scripts d'arrêt du niveau d'exécution actuel, mais seulement ceux pour lesquels il n'y a pas de script de démarrage dans le nouveau niveau d'exécution. Dans cet exemple, ce sont tous les scripts qui résident dans `/etc/init.d/rc3.d` (l'ancien niveau d'exécution était 3) et commencent par un `K`. Le nombre qui suit `K` spécifie l'ordre dans lequel commencer, car il y a certaines relations de dépendance à prendre en considération.

4. Les derniers à démarrer sont les scripts de démarrage du nouveau niveau d'exécution. Ceux-ci sont, dans cet exemple, dans `/etc/init.d/rc5.d` et commencent par un `S`. La même procédure concernant l'ordre dans lequel ils sont démarrés s'applique ici.

Si vous passez au même niveau d'exécution que le niveau d'exécution actuel, init ne vérifie dans `/etc/inittab` que les changements et démarre les étapes appropriées, par exemple, pour démarrer un `getty` sur une autre interface.

7.5 Scripts d'initialisation

Il y a deux types de scripts dans `/etc/init.d` :

Les scripts exécutés directement par init
: Ce n'est le cas que pendant le processus d'amorçage ou si un arrêt immédiat du système est mis en route (lors d'une coupure de courant ou si l'utilisateur appuie sur Ctrl-Alt-Suppr).
: L'exécution de ces scripts est définie dans `/etc/inittab`.

Scripts exécutés indirectement par init
: Ceux-ci sont exécutés lors d'un changement de niveau d'exécution et appellent toujours le script maître `/etc/init.d/rc`, qui garantit l'ordre correct des scripts concernés.

Tous les scripts sont regroupés dans `/etc/init.d`. S'y trouvent également les scripts permettant de changer de niveau d'exécution, qui sont appelés par l'intermédiaire de liens symboliques à partir de l'un des sous-répertoires (`/etc/init.d/rc0.d` vers `/etc/init.d/rc6.d`). Ce n'est que pour des raisons de clarté et cela évite de dupliquer des scripts s'ils sont utilisés dans plusieurs niveaux d'exécution. Comme chaque script peut être exécuté à la fois comme script de démarrage et d'arrêt, ils doivent savoir interpréter les paramètres `start` et `stop`. Les scripts reconnaissent aussi les options `restart`, `reload`, `force-reload` et `status`. Ces différentes options sont décrites dans le tableau 7.2 page suivante. Les scripts qui sont exécutés directement par init n'ont pas ces liens. Ils sont exécutés indépendamment du niveau d'exécutions lorsqu'ils sont nécessaires.

TAB. 7.2: *Options possibles de scripts d'initialisation*

Option	Description
`start`	Démarre le service. Démarrer un service en fonctionnement réussira aussi sans rien faire.
`stop`	Arrête le service.
`restart`	Arrête le service et le redémarre s'il tourne. Dans le cas contraire, le démarre.
`reload`	Recharge la configuration sans arrêter ni redémarrer le service.
`force-reload`	Recharge la configuration si le service le permet. Dans le cas contraire, agit de la même manière que si `restart` avait été indiqué.
`status`	Affiche l'état actuel du service.

Les liens présents dans chaque sous-répertoire associé à un niveau d'exécution permettent d'associer des scripts à différents niveaux d'exécution. Lors de l'installation ou de la désinstallation des paquetages, ces liens sont ajouté et supprimés à l'aide du programme insserv (ou avec `/usr/lib/lsb/install_initd`, un script appelant ce programme). Consultez la page de manuel insserv(8) pour les détails. Vous trouverez ci-après une brève présentation des scripts d'amorçage et d'arrêt lancés en premier ou dernier lieu, respectivement, suivie d'une description du script de maintenance.

`boot` Exécuté lors du démarrage direct du système à l'aide d'init. Il est indépendant du niveau d'exécution choisi et n'est exécuté qu'une fois. Ici; les systèmes de fichiers `proc` et `pts` sont montés et blogd (en anglais, Boot Logging Daemon) est activé. Si le système est amorcé pour la première fois après une mise à jour et une installation, la configuration système initiale est démarrée.

Le démon blogd est un service démarré par les scripts boot et rc avant tout autre. Il est arrêté une fois que les actions déclenchées par les scrips ci-dessus (exécutant un certain nombre de sous-scripts, par exemple) sont achevées. blogd écrit toute sortie écran sur le fichier journal `/var/log/boot.msg`, mais seulement si et quand `/var` est monté en lecture-écriture. Sinon, blogd met en mémoire tampon toutes les données à l'écran jusqu'à ce que `/var` devienne disponible. Vous trouverez plus d'informations au sujet de blogd sur la page de manuel de blogd(8).

Le script `boot` est également chargé de démarrer tous les scripts de `/etc/init.d/boot.d` dont le nom commence par `S`. Les systèmes de fichiers y sont vérifiés et les périphériques de bouclage (loop device) configuré si besoin est. L'horloge système est également réglée. Si une erreur survient lors de la vérification et de la réparation automatiques du système de fichiers, l'administrateur système peut intervenir après la saisir du mot de passe de root. Le dernier script exécuté est `boot.local`.

`boot.local` Saisissez ici des commandes additionnelles pour effectuer un amorçage avant de changer de niveau d'exécution. On peut comparer ce script à `AUTOEXEC.BAT` sur les systèmes DOS.

`boot.setup` Le script est exécuté lors du passage du mode mono-utilisateur à tout autre niveau d'exécution. Il est chargé d'une certain nombre de réglages de base, tels que la disposition du clavier et l'initialisation des consoles virtuelles.

`halt` Ce script n'est exécuté que lors du passage au niveau d'exécution 0 ou 6. Ici, il est exécuté soit en tant que `halt`, soit en tant que `reboot`. La manière dont le système s'arrête ou redémarre dépend de la manière dont `halt` est appelé.

`rc` Ce script appelle les scripts d'arrêt appropriés du niveau d'exécution actuel et les scripts de démarrage du niveau d'exécution qui vient d'être choisi.

7.5.1 Ajouter des scripts d'initialisation

Vous pouvez créer vos propres scripts et les intégrer aisément dans la disposition décrite ci-dessus. Pour des instructions concernant le la mise en forme, le nommage et l'organisation de scripts personnalisés, reportez-vous aux spécifications du LSB ainsi qu'aux pages de manuel init(8), init.d(7) et insserv(8). Consultez en outre les pages de manuel startproc(8) et killproc(8).

Avertissement

Créer vos propres scripts d'initialisation

Des scripts d'initialisation erronés peuvent geler votre machine. Soyez très prudent lorsque vous modifiez ce type de scripts et, dans la mesure du possible, soumettez-les à un test complet dans l'environnement multi-utilisateur. Vous trouverez des informations utiles sur les scripts d'initialisation dans la section 7.3 page 170.

Avertissement

Pour créer un script d'initialisation personnalisé pour un programme ou un service donnés, utilisez le fichier `/etc/init.d/skeleton` comme modèle. Enregistrez une copie de ce fichier sous le nouveau nom et modifiez le programme ainsi que les noms de fichiers, chemins d'accès et tout autre détail pertinent comme nécessaire. Il se peut que vous soyez amené à améliorer le script avec vos propres éléments, de façon à ce que la procédure d'initialisation déclenche les actions correctes.

Le bloc `INIT INFO`, au début du fichier, est un élément obligatoire du script et devra être modifié. Voir l'exemple 7.1 de la présente page.

Example 7.1: *Un bloc INIT INFO minimal*

```
### BEGIN INIT INFO
# Provides:          TOTO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Démarre TOTO pour autoriser XY et fournir YZ
### END INIT INFO
```

Dans la première ligne du bloc `INFO`, après `Provides:`, indiquez le nom du programme ou du service que ce script d'initialisation a sous son contrôle. Dans les lignes `Required-Start:` et `Required-Stop:`, précisez tous les services qui doivent être démarrés ou arrêtés avant que le service lui-même ne soit démarré ou arrêté. Ces informations servent par la suite à générer la numérotation des noms de scripts, comme on les trouve dans les répertoires des niveaux d'exécution. Sous `Default-Start:` et `Default-Stop:`, indiquez les niveaux d'exécution dans lesquels le service devra être automatiquement démarré ou arrêté. Pour finir, sous `Description:`, prévoyez une courte description du service en question.

Pour créer des liens à partir des répertoires des niveaux d'exécution (`/etc/init.d/rc?.d/`) vers les scripts correspondants dans `/etc/init.d/`, saisissez la commande `insserv <nouveau-nom-script>`. Le programme insserv évalue l'en-tête `INIT INFO` pour créer les liens nécessaires pour les scripts de démarrage et d'arrêt dans les répertoires des niveaux d'exécution (`/etc/init.d/rc?.d/`). Le programme veille également à l'ordre correct de démarrage et d'arrêt de chaque niveau d'exécution en ajoutant les nombres nécessaires dans les noms de ces liens. Si vous préférez créer de tels liens avec un

outil graphique, faites appel à l'éditeur de niveaux d'exécution que fournit YaST, comme décrit dans la section 7.6 de la présente page.

Si un script déjà présent dans `/etc/init.d/` doit être intégré dans la disposition existante des niveaux d'exécution, créez les liens dans les répertoires des niveaux d'exécution immédiatement avec insserv ou en activant le service correspondant dans l'éditeur de niveaux d'exécution de YaST. Vos changements seront appliqués lors du prochain redémarrage — le nouveau service sera démarré automatiquement.

Ne définissez pas ces liens manuellement. S'il y a une erreur dans le bloc `INFO`, des problèmes surgiront lorsque, plus tard, `insserv` sera exécuté pour un autre service.

7.6 Éditeur de niveaux d'exécution

Après le démarrage de ce module YaST, s'affiche un aperçu répertoriant tous les services disponibles et l'état actuel de chaque service—indiquant s'ils sont activés. Choisissez si vous préférez utiliser le module en 'Mode simple' ou en 'Mode Experts'. Le 'Mode simple' par défaut devrait suffire pour la plupart des utilisations. La colonne de gauche affiche le nom du service, la colonne du milieu indique son état actuel et la colonne de droite en donne une courte description. Pour le service sélectionné, une description plus détaillée est fournie dans la partie inférieure de la fenêtre; Pour activer un service, sélectionnez-le dans le tableau puis choisissez 'Activer'. Procédez de la même manière pour désactiver un service.

Pour un contrôle détaillé sur les niveaux d'exécution dans lesquels un service est démarré ou arrêté, voire pour changer le niveau d'exécution par défaut, choisissez d'abord 'Mode Experts'. Dans ce mode, la boîte de dialogue affiche dans la partie supérieure le niveau d'exécution par défaut actuel ou "initdefault" (le niveau d'exécution dans lequel le système amorce par défaut). Normalement, le niveau d'exécution par défaut d'un système SUSE LINUX est le niveau d'exécution 5 (mode multi-utilisateur complet avec réseau et XDM). Un autre choix valable pourrait être le niveau d'exécution 3 (mode multi-utilisateur complet avec réseau).

Cette boîte de dialogue de YaST permet de choisir un des niveaux d'exécution (comme répertorié dans le tableau 7.1 page 171) comme le nouveau niveau d'exécution par défaut. Utilisez en outre le tableau de cette fenêtre pour activer ou désactiver un à un des services et des démons. Le tableau donne la liste des services et démons disponibles; montre s'ils sont actuellement activés sur votre système et, si tel est le cas, pour quels niveaux d'exécution. Après avoir sélectionné

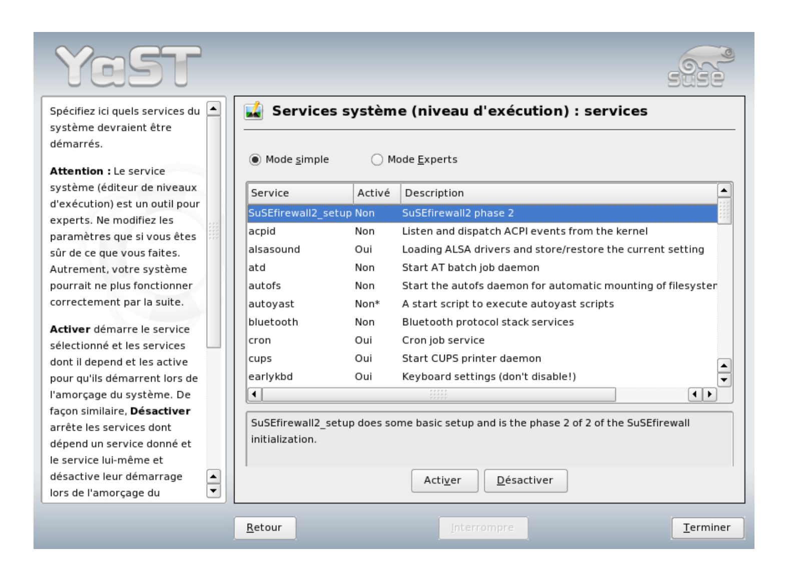


FIG. 7.1: *Éditeur de niveaux d'exécution*

une des lignes à l'aide de la souris, cochez les cases représentant les niveaux d'exécution ('B', '0', '1', '2', '3', '5', '6' et 'S') pour définir les les niveaux d'exécution dans lesquels le service ou le démon sélectionné doit s'exécuter. Le niveau d'exécution 4 n'est pas défini au départ pour permettre de créer un niveau d'exécution personnalisé. Une brève description du service ou du démon actuellement sélectionné est affichée sous le tableau de vue d'ensemble.

Avec 'Démarrer/Arrêter/Actualiser', choisissez si un service doit être activé. 'Actualiser l'état' vérifie l'état actuel. 'Définir/Remettre à zéro' vous permet de choisir s'il faut appliquer vos changements au système ou restaurer les paramètres qui existaient avant de démarrer l'éditeur de niveaux d'exécution. Le fait de choisir 'Terminer' enregistre sur le disque les réglages modifiés.

Avertissement

Changer les réglages des niveaux d'exécution

Un réglage incorrect des niveaux d'exécution peut rendre un système inutilisable. Avant d'appliquer vos changements, soyez absolument sûr d'en connaître les conséquences.

Avertissement

7.7 SuSEconfig et /etc/sysconfig

La configuration principale de SUSE LINUX peut s'effectuer avec les fichiers de configuration qui se trouvent dans `/etc/sysconfig`. Les différents fichiers du répertoire `/etc/sysconfig` ne sont lus que par les scripts pour lesquels ils sont pertinents. Ce comportement garantit que les paramètres du réseau, par exemple, doivent être analysés uniquement par les scripts relatifs au réseau. De nombreux autres fichiers de configuration système sont générés en fonction des réglages de `/etc/sysconfig`. SuSEconfig se charge de cette tâche. Par exemple, si vous modifiez la configuration du réseau, SuSEconfig pourrait également apporter des changements au fichier `/etc/host.conf`, car c'est un des fichiers qui concerne la configuration du réseau.

Si vous modifiez quoi que ce soit dans ces fichiers manuellement, lancez SuSEconfig après pour être sûr que tous les changements nécessaires sont effectués dans tous les endroits pertinents. Si vous modifiez la configuration à l'aide de l'éditeur sysconfig de YaST, tous les changements sont appliqués automatiquement, car YaST démarre automatiquement SuSEconfig pour mettre à jour les fichiers de configuration comme nécessaire.

Ce principe vous permet d'effectuer des changements de base à votre configuration sans avoir à redémarrer le système. Du fait que certains changements sont assez complexes, quelques programmes nécessitent un redémarrage pour que les changements entrent en vigueur. Par exemple, les modifications de la configuration réseau peuvent exiger un redémarrage des programmes réseau concernés. Pour ce faire, vous disposez des commandes `rcnetwork stop` et `rcnetwork start`.

La manière recommandée pour changer la configuration du système se compose des étapes suivantes :

1. Mettez le système en mode mono-utilisateur (niveau d'exécution 1) avec `init 1`.
2. Changez les fichiers de configuration comme nécessaire. Pour cela, utilisez un éditeur de votre choix ou ou l'éditeur de sysconfig de YaST (voir la section 7.8 page suivante).

Avertissement

Changements manuels de la configuration du système

Si vous n'utilisez pas YaST pour modifier les fichiers dans de configuration dans `/etc/sysconfig`, veillez à ce que les valeurs de variables soient représentées par deux guillemets (`KEYTABLE=""`) et à ce que les valeurs contenant des espaces soient entourées de guillemets. Pour les variables composées d'un seul mot, les guillemets sont inutiles.

Avertissement

3. Exécutez `SuSEconfig` pour être sûr que les changements prennent effet. Si vous avez changé les fichiers de configuration avec YaST, cette opération est automatique.
4. Remettez votre système au niveau d'exécution précédent avec une commande comme `init 3` (remplacez `3` par le niveau d'exécution précédent).

Cette procédure est surtout appropriée lorsque vous changez des réglages à l'échelle du système, tels que la configuration du réseau. Les petites modifications ne devraient pas imposer de revenir au mode mono-utilisateur, mais vous pourriez toujours procéder ainsi pour être sûr que tous les programmes concernés sont correctement redémarrés.

Astuce

Configurer la configuration automatique du système

Pour désactiver la configuration automatique du système par SuSEconfig, affectez la valeur `no` à la variable `ENABLE_SUSECONFIG` dans `/etc/sysconfig/suseconfig`. Ne désactivez pas SuSEconfig si vous souhaitez bénéficier de l'assistance à l'installation de SUSE. Il est également possible de désactiver la configuration automatique partiellement.

Astuce

7.8 L'éditeur de sysconfig de YaST

Les fichiers dans lesquels sont enregistrés les réglages les plus importants de SUSE LINUX se trouvent dans le répertoire `/etc/sysconfig`. L'éditeur de sys-

config présente les options d'une manière claire. Les valeurs peuvent être modifiées et ajoutées ultérieurement aux différents fichiers de configuration de ce répertoire. Il n'est en général pas nécessaire de les modifier manuellement, cependant, car ces fichiers sont automatiquement ajustés lors de l'installation d'un paquetage ou de la configuration d'un service.

Avertissement

Modifier les fichiers /etc/sysconfig/*

Ne modifiez pas les fichiers `/etc/sysconfig/*` si vous n'avez pas d'expérience ni de connaissances préalables. Vous pourriez causer des dommages considérables à votre système. Les fichiers présents dans `/etc/sysconfig` contiennent un bref commentaire pour chaque variable pour expliquer quel est leur effet réel.

Avertissement

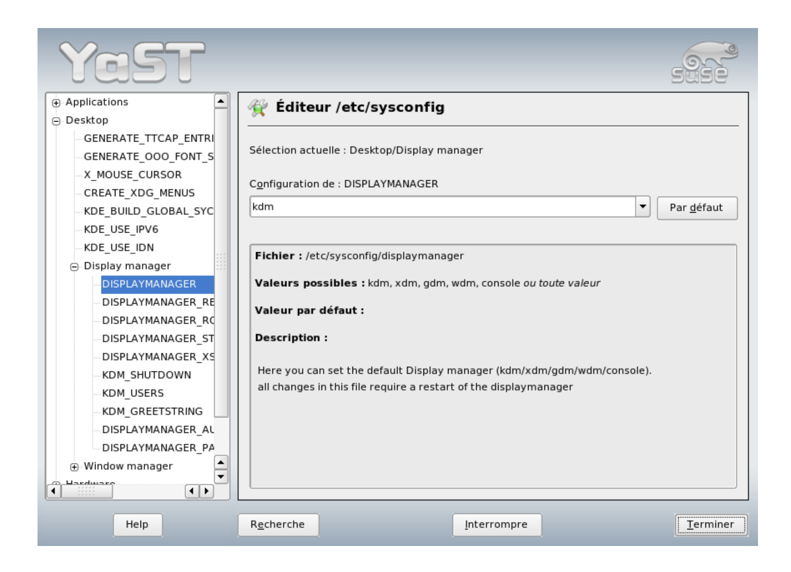


FIG. 7.2: *Configuration du système à l'aide de l'éditeur sysconfig*

La boîte de dialogue sysconfig de YaST est scindée en trois parties. La partie gauche affiche une vue arborescente de toutes les variables que l'on peut configurer. Quand vous sélectionnez une variable, la partie droite affiche à la fois la

sélection actuelle et le réglage actuel de cette variable. Au-dessous, une troisième fenêtre décrit brièvement l'objectif de cette variable, les valeurs possibles, la valeur par défaut et le fichier de configuration réel dont provient cette variable. La boîte de dialogue indique également quel est le script de configuration exécuté après avoir changé la variable et quel est le nouveau service démarré à la suite du changement. YaST vous invite à confirmer vos changements et vous indique quels sont les scripts exécutés une fois que vous avez quitté la boîte de dialogue en choisissant 'Terminer'. Sélectionnez également les services et les scripts à ignorer pour le moment, de façon à ce qu'ils soient démarrés plus tard.

Le gestionnaire d'amorçage

Ce chapitre décrit la façon de configurer GRUB, le gestionnaire d'amorçage utilisé sous SUSE LINUX. Il existe un module de YaST spécial pour effectuer tous les réglages. Si vous n'êtes pas au courant des questions d'amorçage sous Linux, lisez les sections suivantes pour vous informer sur le contexte. Ce chapitre présente également certains des problèmes fréquemment rencontrés lors de l'amorçage avec GRUB ainsi que leur solution.

Ce chapitre est dédié à la gestion de l'amorçage et à la configuration du gestionnaire d'amorçage GRUB. Le processus d'amorçage est décrit dans son ensemble dans le chapitre 7 page 165. Un gestionnaire d'amorçage représente l'interface entre la machine (BIOS) et le système d'exploitation (SUSE LINUX). La configuration du gestionnaire d'amorçage détermine le système d'exploitation qui doit démarrer et ses options.

Les termes suivants apparaîtront souvent dans ce chapitre et des explications sont peut-être nécessaires :

Enregistrement d'amorçage maître La structure du MBR se définit à l'aide d'une convention commune à tous les systèmes d'exploitation. Les 446 premiers octets sont réservés au code du programme. Ils contiennent typiquement le programme du gestionnaire d'amorçage, dans le cas présent GRUB. Les 64 octets suivants prévoient de la place pour une table des partitions contenant jusqu'à quatre sections (voir la section Types de partition page 12). La table des partitions contient des informations sur le partitionnement du disque dur et le type de système de fichiers. Le système d'exploitation a besoin de cette table des partitions pour utiliser les disques durs. Les deux derniers octets du MBR doivent contenir un "nombre magique" fixe (AA55). Un MBR qui contient une autre valeur est considéré comme incorrect par le BIOS et par tous les systèmes d'exploitation sur PC.

Secteurs d'amorçage Les secteurs d'amorçage sont les premiers secteurs des partitions de disque dur, sauf dans le cas de la partition étendue qui ne représente simplement qu'un "conteneur" pour d'autres partitions. Ces secteurs d'amorçage disposent d'une place de 512 octets et sont prévus pour accueillir le code capable d'amorcer un système d'exploitation se trouvant sur cette partition. Ceci s'applique aux secteurs d'amorçage des partitions formatées sous DOS, Windows ou OS/2 qui contiennent aussi d'autres données capitales du système de fichiers. Par opposition, les secteurs d'amorçage des partitions Linux sont, même après l'installation d'un système de fichiers, tout d'abord vides. Une partition Linux ne peut donc pas être *amorcée par elle-même*, même si elle contient un noyau et un système de fichiers racine correct. Un secteur d'amorçage qui contient un code correct pour l'amorçage du système contient dans les 2 derniers octets le même nombre magique que le MBR (AA55).

8.1 Méthodes d'amorçage

Dans le cas le plus simple — si un seul système d'exploitation est installé sur un ordinateur — la gestion de l'amorçage s'effectue comme décrit précédemment. Dès que plus d'un système d'exploitation est installé sur un ordinateur, les méthodes d'amorçage suivantes sont possibles :

Amorcer d'autres systèmes à partir de supports de données externes
Un des systèmes d'exploitation est chargé à partir du disque dur. À l'aide d'un chargeur d'amorçage installé sur un support de données externe (disquette, CD, support de données USB), vous pouvez démarrer les autres systèmes d'exploitation. Étant donné que GRUB peut charger tous les autres systèmes d'exploitation, il n'est pas nécessaire d'utiliser un chargeur d'amorçage externe.

Installer un gestionnaire d'amorçage dans le MBR
Un gestionnaire d'amorçage permet d'avoir plusieurs systèmes d'exploitation en parallèle sur un seul ordinateur et de les utiliser en alternance. Les utilisateurs choisissent le système à charger lors du processus d'amorçage. Un changement de système d'exploitation implique de redémarrer l'ordinateur. La condition préalable est que le gestionnaire d'amorçage choisi s'accorde avec tous les systèmes d'exploitation installés. Le gestionnaire d'amorçage de SUSE LINUX, GRUB, permet d'amorcer tous les systèmes d'exploitation courants. Par défaut, SUSE LINUX installe le gestionnaire d'amorçage souhaité dans le MBR.

8.2 Choix du chargeur d'amorçage

Par défaut, c'est le chargeur d'amorçage GRUB qui est utilisé sous SUSE LINUX. Cependant, pour quelques exceptions et certaines constellations matérielles ou logicielles, il faut avoir recours à LILO. Lorsque vous effectuez une mise à jour à partir d'une version précédente de SUSE LINUX qui utilisait LILO, LILO est à nouveau installé. Lors d'une première installation, au contraire, c'est GRUB qui est installé, à moins que la partition racine ne soit installée sur l'un des systèmes suivants :

- Contrôleur Raid dépendant du processeur (comme, par exemple, de nombreux contrôleurs Promise ou Highpoint)
- Raid logiciel

- LVM

Vous trouverez des informations sur l'installation et la configuration de LILO dans la base de données d'assistance à l'aide du mot-clé *LILO*.

8.3 Amorcer avec GRUB

GRUB (Grand Unified Bootloader) comporte deux niveaux. Le premier niveau (stage1) est stocké sur 512 octets dans le MBR ou le secteur d'amorçage d'une partition de disque ou d'une disquette. Le deuxième niveau (stage 2) est ensuite chargé et contient le véritable code du programme. La seule tâche qu'effectue le premier niveau consiste à charger le deuxième niveau du chargeur d'amorçage.

stage2 peut accéder à des systèmes de fichiers. Actuellement, Ext2, Ext3, ReiserFS, Minix et le système de fichiers DOS FAT utilisé par Windows sont pris en charge. Bien qu'avec des limitations, JFS, XFS ainsi que UFS et FFS, utilisés par les systèmes BSD, sont également pris en charge. Depuis sa version 0.95, GRUB peut également amorcer depuis un CD ou un DVD avec un système de fichiers standard conforme à la norme ISO 9660 selon les spécifications "El Torito". GRUB peut aussi accéder avant le démarrage du système à des systèmes de fichiers de disques pris en charge par le BIOS (disquette ou disques durs, lecteurs de CD ou lecteurs de DVD reconnus par le BIOS). C'est pourquoi il n'est plus nécessaire de réinstaller le chargeur d'amorçage après avoir modifié le fichier de configuration de GRUB (`menu.lst`). À l'amorçage, GRUB relit le fichier de menu contenant les chemins actuels et les déclarations de partitions du noyau ou du disque virtuel initial (`initrd`) et trouve ces fichiers.

Pour la configuration en soi de GRUB, trois fichiers sont nécessaires ; ils sont décrits ci-après :

`/boot/grub/menu.lst` Ce fichier contient toutes les données relatives aux partitions ou aux systèmes d'exploitation qui peuvent être amorcés avec GRUB. Sans ces données, la prise de contrôle du système par le système d'exploitation n'est pas possible.

`/boot/grub/device.map` Ce fichier "traduit" les noms de périphériques utilisés par la notation de GRUB et du BIOS en noms de périphériques Linux.

`/etc/grub.conf` Ce fichier contient les paramètres et options dont l'interpréteur de commandes de GRUB a besoin pour d'installer correctement le chargeur d'amorçage.

GRUB peut être contrôlé de différentes façons. Les choix d'amorçage d'une configuration existante sont sélectionnées à l'aide de l'écran de démarrage (splash screen). La configuration est chargée depuis le fichier `menu.lst`.

GRUB permet la modification de tous les paramètres d'amorçage avant l'amorçage. Par exemple, si une erreur a été faite lors de l'édition du fichier de menu, celui-ci peut être réparé par ce biais. Des commandes d'amorçage peuvent aussi être saisies interactivement dans une sorte d'invite de commande (voir la section Modifier des éléments du menu pendant la procédure d'amorçage page 191). GRUB permet aussi de connaître l'emplacement du noyau et de `initrd` avant l'amorçage. Ainsi, vous pouvez même amorcer un système d'exploitation qui n'a pas été enregistré dans la configuration du chargeur d'amorçage.

Enfin, il existe, avec l'*interpréteur de commandes GRUB*, une émulation de GRUB dans le système installé. Vous pouvez l'utiliser afin d'installer GRUB ou bien pour tester une nouvelle configuration avant de la mettre en place. Voir la section 8.3.4 page 194).

8.3.1 Le menu de démarrage de GRUB

L'écran de bienvenue graphique avec le menu d'amorçage s'appuie sur le fichier de configuration de GRUB `/boot/grub/menu.lst` qui contient toutes les informations à propos des partitions ou des systèmes d'exploitation pouvant être démarrés à l'aide du menu.

GRUB relit à chaque démarrage du système le fichier de menu depuis le système de fichiers. Il n'est donc pas nécessaire de réinstaller GRUB après chaque modification du fichier. Utilisez le module chargeur d'amorçage de YaST pour procéder aux modifications de la configuration de GRUB, comme cela est expliqué dans la section 8.4 page 197.

Le fichier de menu comporte des commandes. La syntaxe est très simple. Chaque ligne comporte une commande, suivie de paramètres optionnels, séparés comme pour l'interpréteur de commandes par des espaces. Quelques instructions admettent pour des raisons historiques un signe égal = avant le premier paramètre. Les commentaires sont introduits par un dièse (#).

Pour identifier les éléments de menu dans l'aperçu du menu, vous devez attribuer un titre (`title`) à chaque choix. Le texte se trouvant après le mot-clé `title`, y compris les espaces, est affiché dans le menu comme une option pouvant être choisie. Toutes les instructions jusqu'au prochain `title` sont exécutées si cette sélection est effectuée dans le menu.

Le cas le plus simple est la redirection vers des chargeurs d'amorçage d'autres systèmes d'exploitation. La commande s'appelle `chainloader` et l'argument est normalement le bloc d'amorçage d'une autre partition dans la notation des blocs (angl. *Block-Notation*) de GRUB, par exemple :

```
chainloader (hd0,3)+1
```

Les noms de périphériques sous GRUB sont expliqués dans la section Conventions de nom pour disques durs et partitions page ci-contre. L'exemple ci-dessus désigne le premier bloc de la quatrième partition sur le premier disque dur.

La commande `kernel` permet d'indiquer une image du noyau. Le premier argument est le chemin vers l'image du noyau sur une partition. Les arguments restants sont transmis au noyau sur la ligne de commande.

Quand le noyau ne dispose pas des pilotes intégrés nécessaires pour l'accès à la partition racine, il faut utiliser `initrd`. Il s'agit là d'une commande GRUB séparée, qui a comme seul argument le chemin vers le fichier `initrd`. Comme l'adresse de démarrage de `initrd` est donnée à l'image du noyau déjà chargée, la commande `initrd` doit suivre directement la commande `kernel`.

La commande `root` permet d'indiquer plus facilement l'emplacement des fichiers du noyau et de initrd. `root` prend un unique argument, soit un périphérique de GRUB, soit une partition sur un tel périphérique. Tout chemin de fichiers du noyau, de `initrd` ou autres, auquel aucun autre périphérique n'a été associé de façon explicite, est associé à ce périphérique jusqu'à la commande `root` suivante. Cette commande n'apparaît pas dans le fichier `menu.lst` qui est généré pendant l'installation. Elle sert à simplifier la modification manuelle.

À la fin de chaque élément de menu, la commande `boot` est toujours implicite, si bien que celle-ci ne doit pas nécessairement être écrite dans le fichier menu. S'il vous arrivait cependant d'utiliser GRUB de façon interactive pour démarrer, vous devez saisir à la fin la commande `boot`. La commande en elle-même n'a pas d'argument. Elle exécute simplement l'image du noyau chargée ou le gestionnaire chaîné indiqué.

Lorsque vous avez écrit tous les éléments du menu, vous devez définir un élément par défaut (`default`). En son absence, le premier (élément `0`) est utilisé. Vous pouvez aussi indiquer un délai en secondes après lequel l'amorçage de l'élément par défaut doit s'effectuer. `timeout` et `default` apparaissent généralement avant les éléments du menu. Vous trouverez un fichier d'exemple et les explications associées dans la section Exemple d'un fichier de menu page suivante.

Conventions de nom pour disques durs et partitions

GRUB utilise pour la désignation de disques durs et de partitions d'autres conventions que celles utilisées pour les périphériques Linux normaux. GRUB numérote les partitions à partir de zéro. Ainsi, (hd0,0) correspond à la première partition sur le premier disque dur. Sur un ordinateur habituel avec un disque connecté comme maître sur le premier contrôleur, le nom du périphérique sous Linux est /dev/hda1.

Les quatre partitions primaires possibles prennent les numéros de partition 0 à 3. Les partitions logiques sont numérotées à partir de 4 :

```
(hd0,0)   première partition primaire sur le premier disque dur
(hd0,1)   deuxième partition primaire
(hd0,2)   troisième partition primaire
(hd0,3)   quatrième partition primaire (et souvent étendue)
(hd0,4)   première partition logique
(hd0,5)   deuxième partition logique
```

GRUB ne différencie pas les périphériques IDE, SCSI ou RAID. Tous les disques durs reconnus par le BIOS ou d'autres contrôleurs sont numérotés conformément à l'ordre d'amorçage préréglé dans le BIOS.

Malheureusement, GRUB ne peut pas établir une correspondance simple en entre les noms de périphériques Linux et les noms de périphériques du BIOS. Il utilise un certain algorithme pour générer cette correspondance et l'enregistre dans le fichier device.map qui peut être modifié si nécessaire. Vous trouverez les informations sur le fichier device.map dans la section 8.3.2 page 193.

Un chemin GRUB complet comprend un nom de périphérique écrit entre parenthèses ainsi que le chemin du fichier dans le système de fichiers sur la partition indiquée. Le chemin commence par une barre oblique (angl. *slash*). Par exemple, sur un système avec un seul disque dur IDE et Linux sur la première partition, le noyau amorçable pourrait se présenter comme suit :

```
(hd0,0)/boot/vmlinuz
```

Exemple d'un fichier de menu

Pour mieux comprendre la structure d'un fichier de menu de GRUB, nous présentons un court exemple. Cet exemple d'installation comprend une partition d'amorçage Linux sous /dev/hda5, une partition racine sous /dev/hda7 et une installation Windows sous /dev/hda1.

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
   kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd

title windows
   chainloader(hd0,0)+1
title disquette
   chainloader(fd0)+1
title failsafe
   kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3
   initrd (hd0,4)/initrd.shipped
```

Le premier bloc concerne la configuration de l'écran de démarrage :

gfxmenu (hd0,4)/message L'image de fond se trouve dans `/dev/hda5` et porte le nom de `message`

color white/blue black/light-gray Le schéma de couleurs : blanc (premier plan), bleu (fond), noir (sélection) et gris clair (fond de la sélection). Le schéma de couleur n'a aucun effet sur l'écran de bienvenue (angl. *splash screen*), uniquement sur le menu modifiable de GRUB dans lequel vous arrivez lorsque vous quittez l'écran de bienvenue à l'aide de Échap.

default 0 Le premier élément du menu avec `title linux` correspond à l'amorçage par défaut.

timeout 8 Après huit secondes sans réaction de la part de l'utilisateur, GRUB amorce le système automatiquement.

Le deuxième bloc, et le plus grand, énumère les différents systèmes d'exploitation amorçables ; les sections de chaque système d'exploitation sont introduites par `title`.

- Le premier élément (`title linux`) s'occupe de l'amorçage de SUSE LINUX. Le noyau (`vmlinuz`) se trouve sur la première partition logique (ici la partition d'amorçage) du premier disque dur. Les paramètres du noyau comme, par exemple, l'indication de la partition racine et du mode VGA y sont rattachés. La partition racine est indiquée selon la convention de nommage de Linux

(/dev/hda7/) puisque cette information est destinée au noyau et n'a rien à voir avec GRUB. initrd se trouve également sur la première partition logique du premier disque dur.

- Le deuxième élément s'occupe du chargement de Windows. Windows est démarré à partir de la première partition du premier disque dur (hd0,0). chainloader +1 gère la lecture et l'exécution du premier secteur de la partition indiquée.
- Le paragraphe suivant a pour but de permettre le démarrage depuis une disquette, sans avoir à modifier le BIOS.
- L'option d'amorçage failsafe sert à démarrer Linux avec un ensemble donné de paramètres du noyau qui permettent d'amorcer Linux même sur des systèmes problématiques.

Le fichier de menu peut être modifié à tout moment. GRUB utilise alors les nouveaux réglages lors de l'amorçage suivant. Éditez ce fichier de façon permanente avec YaST ou avec l'éditeur de votre choix. Sinon, vous pouvez effectuer des modifications temporaires de façon interactive par la fonction d'édition de GRUB. Voir la section Modifier des éléments du menu pendant la procédure d'amorçage de la présente page.

Modifier des éléments du menu pendant la procédure d'amorçage

À partir du menu d'amorçage graphique GRUB, sélectionnez, à l'aide des flèches, le système d'exploitation à amorcer. Si vous choisissez un système Linux, vous pouvez ajouter, à l'invite d'amorçage, vos propres paramètres de démarrage. Si vous appuyez sur Échap et quittez l'écran de bienvenue, vous pouvez, après avoir appuyé sur E, modifier directement et séparément des éléments du menu. Les modifications que vous effectuez de cette manière ne sont valables que pour ce seul processus d'amorçage et ne sont pas conservées de façon durable.

Important

Disposition du clavier pendant le démarrage

Notez que seul la disposition de clavier américain est disponible pour le démarrage.

Important

Une fois le mode d'édition activé, choisissez à l'aide des flèches l'élément du menu dont la configuration est à modifier. Pour pouvoir modifier la configuration, appuyez à nouveau sur E. Corrigez ainsi les erreurs de désignation de partition ou de chemin avant qu'elles n'aient un impact négatif sur le processus de

démarrage. En appuyant sur Entrée, vous quittez le mode d'édition et vous revenez dans le menu. Vous pouvez amorcer cette configuration avec B. D'autres actions possibles sont indiquées dans le texte d'aide en bas.

Si vous voulez enregistrer de façon durable des options de démarrage modifiées et les faire parvenir au noyau, ouvrez en tant qu'utilisateur `root` le fichier `menu.lst` et ajoutez à la ligne existante les paramètres de noyau supplémentaires, séparés par un espace :

```
title linux
   kernel (hd0,0)/vmlinuz root=/dev/hda3 paramètre supplémentaire
   initrd (hd0,0)/initrd
```

GRUB prend en compte automatiquement les nouveaux paramètres lors du démarrage suivant. Sinon, il est aussi possible de faire appel au module chargeur d'amorçage de YaST pour cette modification. Ajoutez les nouveaux paramètres à la ligne existante, séparés par des espaces.

Utilisation de caractères joker pour sélectionner le noyau d'amorçage

Tout particulièrement lorsque vous développez ou utilisez des noyaux personnalisés, vous devez changer les entrées dans `menu.lst` ou modifier la ligne de commande pour être en harmonie avec les noms de noyau et de fichier initrd courants. Afin de simplifier cette procédure, utilisez des *caractères joker* pour mettre à jour dynamiquement la liste de noyaux de GRUB. Toutes les images de noyau qui correspondent à ce schéma spécifique sont alors automatiquement ajoutées à la liste des images amorçables. Veuillez noter qu'il n'y a pas d'assistance technique pour cette fonctionnalité.

Activez l'option caractère joker en créant une entrée de menu supplémentaire dans `menu.lst`. Pour être utiles, toutes les images noyau et initrd doivent avoir un nom de base commun et un identificateur qui correspond au noyau avec son initrd associé. Considérez la configuration suivante :

```
initrd-default
initrd-test
vmlinuz-default
vmlinuz-test
```

Dans ce cas, vous pouvez ajouter les deux images d'amorçage dans une configuration GRUB. Pour avoir les entrées de menu `linux-default` et `linux-test`, l'entrée suivante est nécessaire dans `menu.lst` :

```
title linux-*
   wildcard (hd0,4)/vmlinuz-*
   kernel (hd0,4)/vmlinuz-* root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-*
```

Dans cet exemple, GRUB recherche des entrées qui correspondent au caractère joker dans la partition (hd0,4). Ces entrées sont utilisées pour générer de nouvelles entrées dans le menu GRUB. Dans l'exemple précédent, GRUBse comportera comme si les entrées suivantes existaient dans `menu.lst`:

```
title linux-default
   wildcard (hd0,4)/vmlinuz-default
   kernel (hd0,4)/vmlinuz-default root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-default
title linux-test
   wildcard (hd0,4)/vmlinuz-test
   kernel (hd0,4)/vmlinuz-test root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-test
```

Des problèmes peuvent surgir avec cette configuration si les noms de fichiers ne sont pas utilisés de façon cohérente ou si l'un des fichiers étendus, comme une image initrd, manque.

8.3.2 Le fichier device.map

Le fichier `device.map` contient les correspondances entre les noms de périphériques de GRUB et de Linux. Si vous travaillez sur un système mixte avec des disques durs IDE et SCSI, GRUB doit essayer, à l'aide d'un processus particulier, de déterminer la séquence d'amorçage. GRUB n'a pas accès aux informations du BIOS à ce sujet. GRUB enregistre le résultat de ce contrôle dans `/boot/grub/device.map`. Pour un système particulier, en supposant que la séquence d'amorçage configurée dans le BIOS soit IDE avant SCSI, le fichier `device.map` se présente ainsi :

```
(fd0)  /dev/fd0
(hd0)  /dev/hda
(hd1)  /dev/sda
```

Comme la séquence des disques IDE, SCSI et autres dépend de différents facteurs et que Linux ne peut reconnaître cet ordonnancement, il est possible de configurer la séquence manuellement dans `device.map`. Si vous avez des problèmes

à l'amorçage, vérifiez que l'ordre dans ce fichier correspond à celui du BIOS et, si nécessaire, modifiez-le temporairement avec l'interpréteur de commandes de GRUB décrit dans la section 8.3.4 de la présente page. Si le système Linux est amorcé, vous pouvez modifier de façon durable le fichier `device.map` avec le module chargeur d'amorçage de YaST ou un éditeur de votre choix.

Après modification manuelle de `device.map`, exécutez la commande suivante pour réinstaller GRUB. Avec cette commande, le fichier `device.map` sera lu à nouveau et les commandes contenues dans `grub.conf` seront exécutées :

```
grub --batch < /etc/grub.conf
```

8.3.3 Le fichier /etc/grub.conf

Le troisième fichier de configuration important de GRUB outre `menu.lst` et `device.map` est `/etc/grub.conf`. Les paramètres et les options dont la commande `grub` a besoin pour installer correctement le chargeur d'amorçage y sont énumérés :

```
root (hd0,4)
   install /grub/stage1 d (hd0) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
   quit
```

La signification des différentes choix en détails :

root (hd0,4) Cette commande indique à GRUB de se référer pour les commandes suivantes à la première partition logique du premier disque dur sur lequel il trouve ses fichiers de démarrage.

install `paramètres` La commande `grub` devrait être démarrée avec le paramètre `install`. `stage1` en tant gestionnaire de la première étape d'amorçage doit être installé dans le MBR du premier disque dur (`/grub/stage1 d (hd0)`). `stage2` doit être chargé à l'adresse mémoire 0x8000 (`/grub/stage2 0x8000`). Le dernier élément (`(hd0,4)/grub/menu.lst`) indique à GRUB où se trouve le fichier menu.

8.3.4 L'interpréteur de commandes de GRUB

GRUB existe en fait en deux versions : en tant que gestionnaire d'amorçage, et en tant que programme Linux normal dans `/usr/sbin/grub`. Ce programme

sera désigné par le terme *interpréteur de commandes (*shell*) GRUB*. La fonctionnalité permettant d'installer GRUB comme chargeur d'amorçage sur un disque dur ou sur une disquette est intégrée dans GRUB par le biais des commandes `install` et `setup`. Elle est donc disponible dans l'interpréteur de commandes GRUB lorsque Linux est chargé.

Toutefois, les commandes `setup` et `install` sont également disponibles pendant la procédure d'amorçage avant que Linux ne soit amorcé. Ceci facilite le sauvetage d'un système défectueux qui ne peut plus être amorcé, étant donné que le fichier de configuration défectueux du chargeur d'amorçage peut être évité en saisissant manuellement les paramètres. La saisie manuelle des paramètres au moment de l'amorçage est également intéressante pour tester les nouvelles configurations sans affecter le système original. Saisissez simplement les commandes de configuration expérimentales avec la même syntaxe que dans `menu.lst`. Testez ensuite le bon fonctionnement de ce réglage sans modifier le fichier de configuration existant. Si vous souhaitez, par exemple, tester un nouveau noyau, saisissez la commande `kernel` avec le chemin d'accès au nouveau noyau. Si la procédure d'amorçage échoue, vous reprendrez la prochaine procédure d'amorçage avec le fichier `menu.lst` intact. De la même façon, l'interface en ligne de commande peut aussi servir à amorcer le système malgré un fichier `menu.lst` défectueux en saisissant les paramètres corrigés. Une fois que le système fonctionne, vous pouvez corriger ces paramètres dans `menu.lst` pour rendre système amorçable de façon permanente.

L'algorithme de correspondance entre les périphériques de GRUB et les noms de périphériques de Linux n'entre en jeu que lorsque l'interpréteur de commandes GRUB est utilisé en tant que programme Linux (lancé avec la commande `grub` comme expliqué dans la section 8.3.2 page 193). Pour ce faire, le programme lit le fichier `device.map`. Pour de plus amples informations, voir la section 8.3.2 page 193.

8.3.5 Créer un mot de passe d'amorçage

GRUB prend déjà en charge au moment du démarrage l'accès aux systèmes de fichiers. Les utilisateurs sans droit de super-utilisateur peuvent accéder à des fichiers de votre système Linux auxquels ils n'auraient pas accès une fois le système démarré. Configurez un mot de passe pour bloquer ce genre d'accès ou pour interdire aux utilisateurs d'amorcer certains systèmes d'exploitation.

Pour mettre en place un mot de passe de démarrage, procédez, en tant qu'utilisateur `root`, comme décrit ici :

1. Saisissez la commande `grub` à l'invite de super-utilisateur.
2. Chiffrez le mot de passe dans l'interpréteur de commandes de GRUB :

   ```
   grub> md5crypt
   Password: ****
   Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
   ```

3. Ajoutez la valeur chiffrée dans la section globale du fichier `menu.lst` :

   ```
   gfxmenu (hd0,4)/message
   color white/blue black/light-gray
   default 0
   timeout 8
   password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
   ```

   L'exécution de commandes de GRUB depuis l'invite d'amorçage est protégée. Cette possibilité n'est à nouveau autorisée qu'après avoir saisi (p) ainsi que le mot de passe. Le démarrage d'un système d'exploitation à partir du menu de démarrage reste possible pour tous les utilisateurs.
4. Pour empêcher le démarrage d'un ou de plusieurs systèmes d'exploitation à partir du menu d'amorçage, ajoutez la ligne `lock` dans le fichier `menu.lst` pour chaque section ne devant pas être démarrée sans mot de passe. Par exemple :

   ```
   title linux
   kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd
   lock
   ```

   Après avoir redémarré le système et choisi Linux dans le menu d'amorçage, le message d'erreur suivant apparaît :

   ```
   Error 32: Must be authenticated
   ```

   Appuyez sur (Enter) pour arriver au menu, puis sur (p) pour accéder à l'invite de mot de passe. Après avoir saisi le mot de passe et appuyé sur (Enter), le système d'exploitation désiré (dans ce cas Linux) est amorcé automatiquement.

Important

Mot de passe d'amorçage et écran de démarrage (splash screen)

Si vous utilisez un mot de passe d'amorçage pour GRUB, vous ne disposez pas de l'écran de démarrage habituel.

Important

8.4 Configurer le chargeur d'amorçage avec YaST

La manière la plus simple de configurer le chargeur d'amorçage dans votre système SUSE LINUX est le module de YaST. Dans le Centre de Contrôle de YaST, choisissez 'Système' puis 'Configuration du chargeur d'amorçage'. Vous voyez alors apparaître la configuration actuelle du chargeur d'amorçage dans votre système et vous pouvez procéder à vos modifications (voir figure 8.1 page suivante).

8.4.1 La fenêtre principale

La table contenant les données de configuration se divise en trois colonnes : la colonne de gauche ('Changé') sert à indiquer les options modifiées qui apparaissent dans la colonne du milieu. Pour ajouter une nouvelle option, cliquez sur le bouton 'Ajouter'. Pour changer la valeur d'une option, sélectionnez celle-ci avec la souris puis cliquez sur 'Modifier'. Si vous ne voulez pas utiliser une option existante, sélectionnez-la puis cliquez sur 'Supprimer'. 'Réinitialisation' offre les options suivantes :

Proposer une nouvelle configuration Cette option crée une nouvelle proposition de configuration. Des versions plus anciennes de Linux ou d'autres systèmes d'exploitation, trouvés sur d'autres partitions, sont inclus dans le menu d'amorçage, ce qui vous permet d'amorcer soit Linux, soit l'ancien chargeur d'amorçage. Dans ce second cas, vous accédez à un second menu d'amorçage.

Démarrer de zéro Cette option vous permet de créer votre propre configuration depuis le début sans aucune intervention ou suggestions.

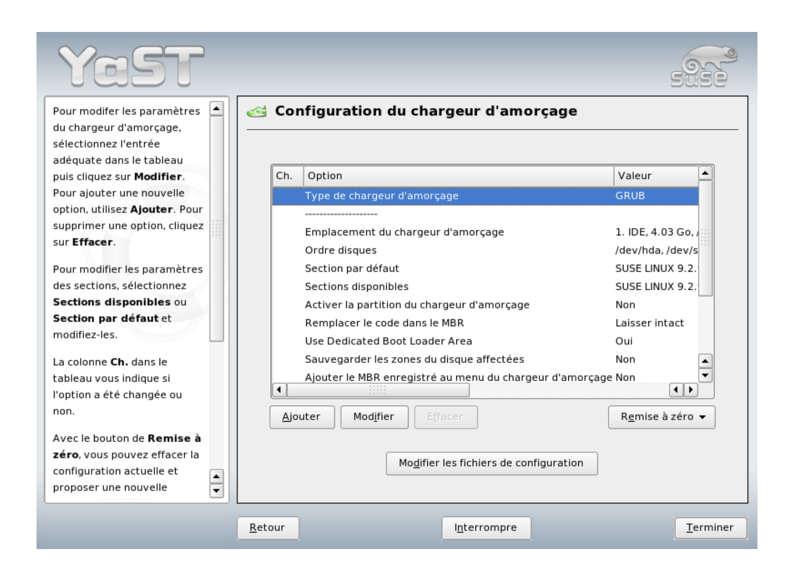


FIG. 8.1: *Configurer le chargeur d'amorçage avec YaST*

Recharger la configuration depuis le disque
Si vous avez déjà procédé à quelques modifications et que celles-ci ne vous conviennent pas, cette option vous permet de revenir à la configuration actuellement enregistrée par votre système.

Proposer et fusionner avec des menus GRUB existants
Si un autre système d'exploitation et une version de Linux plus ancienne sont installés sur d'autres partitions, le menu sera composé d'un choix pour le nouveau SUSE LINUX, un choix pour l'autre système d'exploitation ainsi que tous les choix de l'ancien menu d'amorçage. Ce processus peut prendre un certain temps. Si vous utilisez LILO, cette option n'existe pas.

Restaurer le MBR depuis le disque dur
Avec cette option, vous reprenez le MBR enregistré sur le disque dur.

Choisissez 'Modifier les fichiers de configuration' pour modifier directement les fichiers de configurations dans un éditeur. Sélectionnez le fichier dans le champ de sélection pour l'éditer directement. Cliquez sur 'OK' et les changements seront enregistrés. Utilisez 'Annuler' pour sortir de la configuration du chargeur d'amorçage sans l'enregistrer et 'Retour' pour revenir à la fenêtre principale.

8.4.2 Options de la configuration du chargeur d'amorçage

La configuration avec YaST est beaucoup plus simple que la modification directe des fichiers. Choisissez une option avec la souris et cliquez sur 'Modifier'. Une boite de dialogue apparaît dans laquelle vous pouvez procéder à des réglages individuels. Cliquez sur 'OK' pour confirmer les modifications et retourner à la page principale dans laquelle vous pourrez modifier d'autres options. Ces options sont différentes selon le chargeur d'amorçage. Nous vous présentons ici quelques options importantes de GRUB :

Type de chargeur d'amorçage Avec cette option, vous pouvez passer de GRUB à LILO et réciproquement. Vous ouvrez ainsi une autre page dans laquelle vous pouvez indiquer le type de changement. Vous pouvez transformer la configuration de GRUB en une configuration LILO similaire, en risquant toutefois de perdre quelques informations au cas où il n'existerait pas d'options équivalentes. En outre, vous pouvez créer une configuration totalement nouvelle ou accepter une proposition que vous pourrez bien entendu modifier si vous le désirez.

Si vous démarrez la configuration du chargeur d'amorçage dans le système en fonctionnement, vous pouvez charger la configuration sur le disque dur. Néanmoins, si vous décidez de revenir au chargeur d'amorçage précédemment configuré, vous pouvez le charger à nouveau en utilisant la dernière option de cette configuration. Cependant, tout ceci n'est possible que tant que vous n'avez pas quitté le module du chargeur d'amorçage.

Emplacement du chargeur d'amorçage
Indiquez dans cette page où le chargeur d'amorçage doit être installé : dans le secteur maître d'amorçage (MBR), dans le secteur d'amorçage de la partition d'amorçage (si elle existe déjà), dans le secteur d'amorçage de la partition racine ou sur la disquette. Avec l'option 'Autres', vous pouvez choisir le lieu d'installation librement.

Ordre des disques durs Si vous disposez de deux ou plusieurs disques durs, indiquez ici l'ordre correspondant à celui de la configuration du BIOS.

Section par défaut Avec cette option, vous précisez le noyau ou système d'exploitation qui doit démarrer par défaut. Une fois que le délai d'attente est passé, ce système sera amorcé automatiquement. Dans ce menu, vous verrez une liste de tous les choix du menu d'amorçage en cliquant sur le bouton 'Modifier'. Choisissez une des entrées de la liste, et activez là en cliquant sur le bouton 'Definir comme valeur par défaut'. Ici, vous avez aussi la possibilité de modifier une entrée en cliquant sur 'Modifier'.

Sections disponibles Dans la fenêtre principale, cette option vous permet de voir quels choix de menu existent. Si vous choisissez cette option et cliquez sur 'Changer', vous ouvrirez la même page qu'avec 'Sélection par défaut'.

Activer la partition du chargeur d'amorçage
Utilisez cette option pour activer la partition dont le secteur d'amorçage contient le chargeur d'amorçage, indépendamment de la partition sur laquelle se trouve le répertoire contenant les fichiers du chargeur d'amorçage (`/boot` ou le répertoire racine `/`).

Remplacer le code dans le MBR Si vous aviez installé GRUB directement dans le secteur maître d'amorçage (MBR) ou si vous procédez à une installation sur un disque dur neuf et que vous ne souhaitiez plus installer GRUB dans le secteur maître d'amorçage, remettez en place le code d'amorçage générique à l'aide de cette option.

Sauvegarde des fichiers et zones du disque dur
Les zones du disque dur qui ont été modifiées sont sauvegardées.

Ajouter le MBR enregistré dans le menu du chargeur d'amorçage
Ajoute le MBR enregistré dans le menu du chargeur d'amorçage.

Utilisez l'option 'Time-out' pour définir le délai d'attente du chargeur d'amorçage (durée pendant laquelle le chargeur attend une saisie au clavier avant de démarrer le système par défaut). Le bouton 'Ajouter' permet de définir toute une série d'autres options. Pour obtenir plus de détails quant aux options possibles, vous pouvez vous référer aux pages de manuel respectives 'grub(8) ou lilo(8)) et à la documentation en ligne disponible à l'adresse suivante :`http://www.gnu.org/software/grub/manual/`.

8.5 Désinstallation du chargeur d'amorçage Linux

YaST peut procéder à la désinstallation du chargeur d'amorçage de Linux et à la restauration du MBR dans l'état qu'il avait avant l'installation de Linux. Lors de l'installation, YaST génère automatiquement une copie de sauvegarde du MBR original et, si vous le souhaitez, l'applique à nouveau, écrasant ainsi GRUB.

Pour désinstaller GRUB, démarrez le module du chargeur d'amorçage de YaST ('Système' → 'Configuration du chargeur d'amorçage'). Dans la première boîte de

dialogue, sélectionnez 'Remise à zéro' → 'Restaurer le MBR du disque dur' puis quittez avec 'Terminer'. Dans le MBR, GRUB est écrasé avec les données du MBR d'origine.

8.6 Créer des CD d'amorçage

Si vous rencontrez des problèmes pour démarrer votre système avec un gestionnaire d'amorçage ou si vous ne pouvez pas installer le chargeur d'amorçage dans le secteur maître d'amorçage (MBR) de votre disque dur ni sur une disquette, vous pouvez aussi créer un CD amorçable sur lequel sont gravés tous les fichiers nécessaires au démarrage de Linux. Votre ordinateur doit pour cela disposer d'un graveur de CD correctement installé.

Pour créer un CD-ROM d'amorçage avec GRUB, vous n'avez besoin que de `stage2_eltorito`, une forme spéciale de *stage2* et éventuellement d'un `menu.lst` optionnel adapté à vos besoins. Les fichiers classiques `stage1` et `stage2` ne sont pas nécessaires.

Créez un répertoire dans lequel l'image ISO sera créée. par exemple avec les commandes `cd /tmp` et `mkdir iso`. Créez aussi un sous-répertoire pour GRUB à l'aide de `mkdir -p iso/boot/grub`. Copiez le fichier `stage2_eltorito` dans le répertoire `grub` :

```
cp /usr/lib/grub/stage2_eltorito iso/boot/grub
```

Copiez également le noyau (`/boot/vmlinuz`), `initrd` (`/boot/initrd`) et `/boot/message` dans `iso/boot/` :

```
cp /boot/vmlinuz iso/boot/
cp /boot/initrd iso/boot/
cp /boot/message iso/boot/
```

Pour que GRUB puisse trouver ces fichiers, copiez le fichier `menu.lst` dans `iso/boot/grub` et modifiez les chemins d'accès de façon à les faire pointer sur le lecteur de CD-ROM. Pour cela, remplacez dans les chemins d'accès le noms de périphérique des disques durs, de la forme `(hd*)`, par le nom de périphérique du lecteur de CD-ROM, `(cd)` :

```
gfxmenu (cd)/boot/message
timeout 8
default 0

title Linux
    kernel (cd)/boot/vmlinuz root=/dev/hda5 vga=794 resume=/dev/hda1
splash=verbose showopts
    initrd (cd)/boot/initrd
```

Enfin, créez une image ISO à l'aide de la commande suivante :

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso iso
```

Gravez le fichier obtenu `grub.iso` sur un CD avec le programme de votre choix.

8.7 L'écran graphique de SUSE

Depuis SUSE LINUX 7.2, l'écran graphique de SUSE est affiché sur le premier terminal si l'on utilise l'option "vga=<valeur>" comme paramètre du noyau. Si vous installez avec YaST, cette option est activée automatiquement en fonction de la résolution choisie et de la carte graphique. Il y a trois manières de désactiver l'écran de SUSE :

Désactiver l'écran de SUSE lorsque c'est nécessaire.
Pour désactiver l'écran graphique, tapez la commande `echo 0 >/proc/splash` dans la ligne de commande. Pour l'activer à nouveau, tapez `echo 1 >/proc/splash`.

Désactiver l'écran de SUSE par défaut.
Ajoutez le paramètre de noyau `splash=0` à la configuration de votre gestionnaire d'amorçage. Le chapitre 8 page 183 fournit plus d'informations pour ce réglage. Toutefois, si vous préférez le mode texte, qui était le mode par défaut dans les versions plus anciennes, réglez le paramètre `vga=normal`.

Désactiver complètement l'écran de SUSE.
Compilez un nouveau noyau et désactivez l'option 'Use splash screen instead of boot logo' dans 'framebuffer support'.

Astuce

Le fait de désactiver la prise en charge du framebuffer dans le noyau supprime aussi automatiquement l'écran de bienvenue. SUSE ne peut fournir aucune assistance pour votre système si vous l'utilisez avec un noyau personnalisé.

Astuce

8.8 Dépannages

Cette section répertorie quelques uns des principaux problèmes qui peuvent surgir lors de l'amorçage avec GRUB. Les solutions possibles sont abordées. Pour certaines, vous trouverez un article dans la base de données support (`http://portal.suse.de/sdb/de/index.html`). Si votre problème n'est pas contenu dans cette liste, nous vous conseillons de faire une recherche dans la base de données support (`https://portal.suse.com/PM/page/search.pm`) avec les mots-clés *GRUB*, *Amorcer*, *Chargeur d'amorçage*.

GRUB et XFS XFS ne laisse aucune place dans le bloc d'amorçage de la partition pour `stage1`. Il est donc important de ne pas choisir comme emplacement pour un chargeur d'amorçage une partition sur laquelle se trouve un XFS. Ce problème peut être résolu en créant une partition d'amorçage séparée qui ne soit pas formatée avec XFS.

GRUB et JFS Bien que techniquement possible, une combinaison de GRUB avec JFS est problématique. Dans ce cas, créez une partition d'amorçage séparée (`/boot`) et formatez-la avec Ext2. Installez GRUB dans cette partition.

GRUB indique une erreur GRUB Geom Error
GRUB contrôle la géométrie des disques durs rattachés au moment de l'amorçage. Dans certains cas, le BIOS fournit des indications incohérentes, si bien que GRUB indique une erreur GRUB Geom Error. Dans de tels cas, utilisez LILO ou mettez le BIOS à jour. Vous trouverez des informations détaillées sur l'installation, la configuration et la maintenance de LILO dans la base de données d'assistance à l'aide du mot-clé LILO.

GRUB donne ce message d'erreur également lorsque Linux est installé dans le système sur un disque dur supplémentaire qui n'est pas enregistré dans le BIOS. La première partie du chargeur d'amorçage (*stage1*) est trouvée et chargée correctement mais la deuxième partie (*stage2*) n'est pas trouvée. La solution est alors d'enregistrer le nouveau disque dur dans le BIOS.

Le système contenant des disques durs IDE et SCSI n'amorce pas

Il peut arriver que, lors de l'installation, YaST ait mal reconnu l'ordre d'amorçage des disques durs (et que vous ne l'ayez pas corrigé). Ainsi, GRUB prendra, par exemple, `/dev/hda` comme `hd0` et `/dev/sda` comme `hd1` alors que dans le BIOS, c'est l'ordre inverse (SCSI *avant* IDE) qui est entré.

Dans ce cas, corrigez, lors de l'amorçage, les disques durs utilisés à la ligne de commande GRUB puis modifiez le fichier `device.map` dans le système amorcé afin de corriger les correspondances une bonne fois pour toutes. Ensuite, vérifiez également les noms de périphériques GRUB dans les fichiers `/boot/grub/menu.lst` et `/boot/grub/device.map` et installer avec le chargeur d'amorçage à nouveau avec la commande suivante :

```
grub --batch < /etc/grub.conf
```

Amorcer Windows depuis le deuxième disque dur

Certains systèmes d'exploitation, par exemple Windows, ne peuvent démarrer qu'à partir du premier disque dur. Lorsque vous avez installé un tel système d'exploitation sur un disque dur autre que le premier, vous pouvez exécuter un échange logique dans l'élément de menu correspondant.

```
...
title windows
map (hd0) (hd1)
map (hd1) (hd0)
chainloader(hd1,0)+1
...
```

Dans cet exemple, Windows démarre à partir du deuxième disque dur. Pour cela, la séquence logique des disques durs est modifiée avec `map`. Durant cet échange, la logique du fichier du menu de GRUB n'est pas modifiée. Ainsi, vous devrez indiquer le deuxième disque dur dans `chainloader`.

8.9 Pour de plus amples informations

Vous trouverez des informations détaillées sur GRUB, en anglais, à l'adresse `http://www.gnu.org/software/grub/`. Si texinfo est installé sur votre ordinateur, vous pouvez afficher les pages Info relatives à GRUB dans un

terminal avec `info grub`. Recherchez aussi dans la base de données d'assistance `http://portal.suse.com/sdb/en/index.html` le mot-clé "GRUB" afin de trouver des informations sur des thèmes particuliers.

Le noyau Linux

Le noyau gère le matériel du système Linux et le met à la disposition des différents processus. Dans les pages qui suivent, vous ne deviendrezcertes pas un "bidouilleur" (hacker) du noyau, mais vous apprendrez à mettre à jour le noyau et à compiler puis à installer un noyau personnalisé. Si vous procédez comme le décrit ce chapitre, le noyau précédent reste opérationnel et peut être amorcé à tout moment si c'est nécessaire.

Le noyau placé lors de l'installation dans le répertoire `/boot` est configuré de manière à prendre en charge une large gamme de matériel. Il n'est généralement pas nécessaire de compiler votre propre noyau, sauf si vous voulez essayer des fonctionnalités ou des pilotes expérimentaux.

Il est souvent possible de modifier le comportement du noyau installé à l'aide de paramètres de noyau. Par exemple, le paramètre `desktop` diminue les tranches de temps de l'ordonnanceur ce qui rend le système subjectivement plus rapide. Vous trouverez plus d'informations dans la documentation relative au noyau qui se trouve dans le répertoire `/usr/src/linux/Documentation` si le paquetage `kernel-source` est installé.

Plusieurs `Makefiles` sont fournies avec le noyau pour automatiser la procédure. Choisissez les paramètres du matériel et les autres fonctionnalités du noyau. Comme vous devez assez bien connaître votre système informatique pour faire les bons choix, nous vous recommandons pour votre première tentative de modifier un fichier de configuration existant et fonctionnel.

9.1 Mise à jour du noyau

Pour installer une mise à jour officielle du noyau SUSE, utilisez la fonctionnalité de mise à jour en ligne de YaST. Après une mise à jour du noyau, vous devrez réamorcer votre système car l'ancien noyau toujours en cours d'exécution ne trouvera pas de modules appropriés pour assurer les fonctions nécessaires. Vous trouverez plus d'informations à propos de la mise à jour en ligne avec YaST à la section 2.2.3 page 50.

Lorsque vous effectuez la mise à jour, une fenêtre apparaîtra pour vous expliquer toutes les actions nécessaires. Suivez ces indications pour garder un système cohérent.

9.2 Les sources du noyau

Pour compiler un noyau, vous devez installer le paquetage `kernel-source`.YaST établit automatiquement une liste d'autres paquetages à installer, comme le compilateur C (paquetage `gcc`), les binutils de GNU (paquetage `binutils`) et les fichiers d'en-têtes pour le compilateur C (paquetage `glibc-devel`). Ces autres paquetages devront également être installés.

Une fois l'installation terminée, les sources du noyau se trouvent dans le répertoire /usr/src/linux-<version-noyau>. Si vous projetez de faire des tests avec le noyau et d'en maintenir différentes versions en même temps sur votre disque, décompactez les diverses versions dans différents répertoires et créez un lien symbolique vers la source du noyau actuelle. Comme certains paquetages s'attendent à ce que les sources se trouvent dans /usr/src/linux, assurez-vous que ce répertoire est un lien vers la source du noyau actuelle. YaST se charge de cela automatiquement.

9.3 Configuration du noyau

La configuration du noyau en cours d'exécution est enregistrée dans le fichier /proc/config.gz. Pour modifier cette configuration, allez dans le répertoire /usr/src/linux en tant que root et lancez les commandes suivantes :

```
zcat /proc/config.gz > .config
make oldconfig
```

La commande make oldconfig utilise le fichier /usr/src/linux/.config comme base de la configuration du noyau actuelle. Lorsque de nouvelles options apparaissent dans le noyau courant, elles peuvent alors être choisies ou non. Lorsque le fichier .config est absent, une configuration par défaut contenue dans les sources du noyau est utilisée.

Il n'est pas possible de couvrir ici en détail les diverses possibilités de configuration du noyau. Faites appel à la pléthore de fichiers d'aide qui existent sur le sujet. La version la plus récente de la documentation se trouve toujours dans le répertoire /usr/src/linux/Documentation.

9.3.1 Configuration depuis la ligne de commande

Pour configurer le noyau, allez dans le répertoire /usr/src/linux et saisissez la commande make config. Choisissez les fonctionnalités que vous désirez que le noyau prenne en charge. Deux ou trois possibilités s'offrent généralement à vous lorsque vous répondez aux questions : Y (yes - oui), N (no - non) et M (module). M signifie que le pilote correspondant n'est pas compilé directement dans le noyau, mais chargé en tant que module. Les pilotes nécessaires à l'amorçage du système doivent être liés physiquement au noyau ; vous choisirez donc

dans ce cas Y. Avec Entrée, confirmez la présélection présente dans le fichier `.config`. Si vous appuyez sur une autre touche lors d'une question, vous obtenez l'affichage d'un court texte d'aide sur l'option concernée.

9.3.2 Configuration en mode texte

menuconfig permet de configurer le noyau de manière plus confortable. Vous devrez éventuellement installer avec YaST le paquetage `ncurses-devel`. Démarrez la configuration du noyau avec la commande `make menuconfig`.

Pour ne modifier que légèrement la configuration, il n'est pas nécessaire de passer toutes les questions. Utilisez plutôt le menu pour accéder à certaines sections directement. Les réglages par défaut sont chargés à partir du fichier `.config`. Pour charger une autre configuration, choisissez 'Load an Alternate Configuration File' et indiquez le nom du fichier.

9.3.3 Configuration avec le système X Window

Si vous avez installé et configuré le système X Window (paquetage `xorg-x11`) ainsi que les paquetages de développement QT (`qt3-devel`), vous pouvez utiliser la commande `make xconfig` pour accéder à une interface utilisateur graphique pour la configuration. Si vous n'êtes pas connecté en tant que `root` au système X Window, exécutez la commande `sux` pour obtenir un interpréteur de commandes en tant que `root` avec accès à l'affichage. Les paramètres par défaut sont chargés à partir du fichier `.config`. Comme la configuration avec `make xconfig` n'est pas aussi bien maintenue que les autres possibilités de configuration, lancez la commande `make oldconfig` après avoir utilisé cette méthode de configuration.

9.4 Modules du noyau

Les composants matériels des PC sont nombreux et variés. Pour pouvoir les utiliser correctement, vous aurez besoin d'un "pilote" qui permettra au système d'exploitation (sous Linux, le noyau) d'accéder à ce matériel. Il y a en gros deux mécanismes pour intégrer des pilotes au noyau :

- Les pilotes peuvent être compilés directement dans le noyau. Dans ce guide, de tels noyaux ("d'un seul bloc") sont qualifiés de noyaux *monolithiques*. Certains pilotes ne peuvent être utilisés que sous cette forme.

- Les pilotes peuvent n'être chargés dans le noyau qu'en fonction des besoins. On qualifie dans ce cas le noyau de *modulaire*. L'avantage est que seuls les pilotes nécessaires sont chargés et que le noyau ne contient aucun élément inutile.

Lors de la configuration du noyau, on établit quels pilotes sont liés physiquement au noyau et lesquels sont placés dans des modules. Tous les composants du noyau qui ne sont pas impérativement nécessaires au cours du processus d'amorçage devraient être compilés sous forme de modules. On s'assure ainsi que le noyau n'est pas trop volumineux et qu'il peut être chargé sans difficulté à partir du BIOS et de n'importe quel gestionnaire d'amorçage. Les pilotes pour `ext2`, les pilotes SCSI pour un système SCSI et d'autres fonctionnalités similaires doivent être directement compilés au sein du noyau. Inversement, la prise en charge d'`isofs`, de `msdos` ou du son (`sound`), qui ne sont pas nécessaires au démarrage de l'ordinateur, devraient toujours être compilées sous forme de modules.

Astuce

Vous pouvez même fabriquer des modules pour les pilotes nécessaires à l'amorçage du système. Dans ce cas, le disque virtuel initial est utilisé pour charger ces modules à l'amorçage.

Astuce

Les modules du noyau se trouvent dans le répertoire `/lib/modules/<version>`. `version` correspond à la version du noyau en cours d'exécution.

9.4.1 Reconnaissance du matériel à l'aide de hwinfo

Le programme hwinfo à votre disposition sous SUSE LINUX permet de reconnaître le matériel actuellement présent sur l'ordinateur et de choisir les pilotes servant à gérer ce matériel. La commande `hwinfo --help` vous offre un court paragraphe d'aide. Par exemple, pour obtenir des informations sur les périphériques SCSI installés, saisissez la commande `hwinfo --scsi`. Toutes ces informations sont également disponibles dans le module d'informations sur le matériel de YaST.

9.4.2 Manipulation des modules

Vous trouverez les utilitaires pour charger les modules dans le noyau dans le paquetage `module-init-tools`. Vous y trouverez les commandes suivantes :

insmod insmod charge le module indiqué après l'avoir recherché dans un sous-répertoire de /lib/modules/<version>. Il est toutefois conseillé d'utiliser modprobe à la place de insmod car modprobe vérifie également les dépendances du module.

rmmod Le module indiqué est déchargé. Cela n'est bien sûr possible que si la fonctionnalité correspondante du noyau n'est plus utilisée. Par conséquent, il n'est pas possible de décharger le module isofs lorsqu'un un CD est encore monté.

depmod Crée le fichier modules.dep dans le répertoire /lib/modules/<version> qui définit les dépendances entre tous les modules. C'est nécessaire pour s'assurer que lors du chargement de modules, tous les modules qui en dépendent sont également chargés. Ce fichier est généré au démarrage du système s'il n'existe pas.

modprobe Charge ou décharge un module en prenant en compte les dépendances de ce module. Cette commande est très puissante et permet de faire de nombreuses choses comme essayer tous les modules d'un certain type, jusqu'à réussir à charger l'un d'entre eux. Contrairement au chargement au moyen d'insmod, modprobe analyse le fichier /etc/modprobe.conf et on devrait donc en principe l'employer pour charger des modules. Pour des informations détaillées à ce sujet, consultez les pages de manuel appropriées.

lsmod Indique quels sont les modules actuellement chargés et par combien d'autres modules ils sont utilisés. Les modules qui ont été chargés par le démon du noyau sont identifiés par l'étiquette autoclean. Cette étiquette signale que ces modules seront automatiquement retirés s'ils restent inutilisés pendant un certain temps.

modinfo Affiche des informations sur un module. Étant donné que ces informations sont extraites du module, seules les informations qui ont été intégrées par les développeurs du pilote pourront être affichées. Les informations peuvent contenir l'auteur, une description, la licence, les paramètres de module, les dépendances et les alias.

9.4.3 /etc/modprobe.conf

Le chargement des modules est influencé par les fichiers /etc/modprobe.conf et /etc/modprobe.conf.local, ainsi que par le répertoire /etc/modprobe.d.Reportez-vous à la page de manuel man modprobe.conf. On trouve également dans ce fichier les paramètres des modules qui accèdent directement au

matériel. Les modules de ce type, par exemple pour un lecteur CD-ROM ou un pilote réseau, peuvent nécessiter des options spécifiques au système. Les paramètres utilisés sont décrits dans les sources du noyau. Installez le paquetage `kernel-source` et lisez la documentation contenue dans le répertoire `/usr/src/linux/Documentation`.

9.4.4 Kmod — le chargeur de modules du noyau

Le chargeur de modules du noyau est la méthode la plus élégante d'utiliser les modules. Kmod veille en arrière-plan à ce que les modules nécessaires soient automatiquement chargés au moyen d'appels à modprobe dès que l'on accède à la fonctionnalité correspondante du noyau.

Pour utiliser Kmod, cochez l'option 'Kernel module loader' (`CONFIG_KMOD`) lors de la configuration du noyau. Kmod n'est pas conçu pour décharger les modules automatiquement. Si l'on considère la quantité de mémoire vive (RAM) actuellement installée dans les ordinateurs, le gain de mémoire serait marginal.

9.5 Compiler le noyau

► **x86, AMD64, EM64T**
Nous recommandons de générer une ”bzImage“. Ainsi, on peut en général éviter que le noyau ne devienne trop volumineux, comme cela peut facilement se produire lorsque l'on choisit trop de fonctionnalités et qu'on crée une ”zImage“. Vous obtenez alors des messages comme kernel too big ou System is too big. ◄

Après avoir personnalisé la configuration de votre noyau comme décrit à la section 9.3 page 209, démarrez la compilation (souvenez-vous d'aller d'abord dans le répertoire `/usr/src/linux/`) :

```
make clean
make bzImage
```

Vous pouvez également saisir ces deux commandes sur une seule ligne de commande :

```
make clean bzImage
```

Après une compilation réussie, vous trouverez le noyau compressé dans `/usr/src/linux/arch/<arch>/boot`. L'image du noyau — le fichier qui contient le noyau — s'appelle `bzImage`.

Si vous ne trouvez pas ce fichier, il est très probable qu'une erreur soitapparue au cours de la compilation du noyau. Si vous êtes sous Bash, vous pouvez démarrer à nouveau le processus de compilation et en obtenir un "enregistrement simultané" dans le fichier `kernel.out` :

```
make bzImage V=1 2>&1 | tee kernel.out
```

Si vous avez configuré des parties du noyau sous forme de modules pouvant être chargés, vous devez ensuite passer à la compilation de ces modules. Utilisez pour ce faire la commande `make modules`.

9.6 Installer le noyau

Après avoir compilé le noyau, vous devez l'installer afin de pouvoir l'amorcer. Vous devez installer le noyau dans le répertoire `/boot`. Saisissez pour cela la commande suivante :

```
INSTALL_PATH=/boot make install
```

Les modules compilés doivent encore être installés. Saisissez `make modules_install` pour les installer dans les bons répertoires cibles dans `/lib/modules/<version>`. Si la version de l'ancien noyau est la même, les anciens modules sont écrasés. Mais vous pouvez réinstaller les modules et le noyau d'origine à partir des CD.

Astuce

Veillez à ce que les modules éventuels correspondants à des fonctionnalités que vous venez de compiler directement dans le noyau aient été retirés du répertoire `/lib/modules/<version>`. C'est une des raisons pour lesquelles il est *fortement* déconseillé aux utilisateurs inexpérimentés de compiler le noyau.

Astuce

Afin que GRUB puisse amorcer l'ancien noyau (désormais `/boot/vmlinuz.old`), ajoutez dans le fichier `/boot/grub/menu.lst` une nouvelle image

d'amorçage intitulée Linux.old. Cette procédure est décrite en détail dans le chapitre 8 page 183. GRUB ne nécessite pas d'être réinstallé.

Le fichier /boot/System.map contient les symboles du noyau requis par les modules pour pouvoir appeler correctement les fonctions du noyau. Ce fichier dépend du noyau en cours de fonctionnement. C'est pourquoi, après avoir compilé et installé le noyau, vous devez copier le nouveau fichier /usr/src/linux/System.map dans le répertoire /boot. Ce fichier sera généré à chaque compilation du noyau. Si lors de l'amorçage, vous recevez un message d'erreur comme System.map does not match actual kernel, il est alors probable que vous ayiez oublié de copier le fichier System.map dans /boot après la compilation du noyau.

9.7 Faire le ménage sur le disque dur après la compilation

Si vous avez des problèmes d'espace disque, vous pouvez supprimer les fichiers objets produits pendant la compilation du noyau avec make clean. Si toutefois vous disposez de l'espace disque suffisant et prévoyez de configurer à nouveau le noyau à maintes reprises, ignorez cette dernière étape. Une nouvelle compilation du noyau est alors beaucoup plus rapide, puisque seules les parties concernées par les modifications sont recompilées.

Particularités de SUSE LINUX

Vous trouverez dans ce chapitre des informations sur les différents paquetages logiciels ainsi que sur les consoles virtuelles et la disposition du clavier. En conclusion, vous trouverez une section consacrée aux adaptations locales et linguistiques (I18N et L10N).

10.1 Informations relatives à certains paquetages logiciels spéciaux

10.1.1 Le paquetage bash et /etc/profile

Le programme bash lit et évalue dans cet ordre les fichiers d'initialisation lorsqu'il est appelé comme interpréteur de commandes à la connexion (shell de login) :

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Les utilisateurs peuvent ajouter leurs propres lignes dans `~/.profile` ou dans `~/.bashrc`. Pour modifier ces fichiers comme il se doit, il est indispensable de recopier les paramètres de base de `/etc/skel/.profile` ou de `/etc/skel/.bashrc` dans le répertoire utilisateur. Il est donc recommandé, après avoir effectué une mise à jour, de copier la configuration à partir de `/etc/skel`. Exécutez les commandes suivantes depuis un terminal afin de conserver une copie des modifications que vous avez réalisées :

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Vous devez alors copier vos adaptations personnelles depuis les fichiers `*.old`.

10.1.2 Le paquetage cron

Les tables `cron` se trouvent maintenant dans `/var/spool/cron/tabs`. Le fichier `/etc/crontab` sert de planificateur horaire pour tout le système. Entrez le nom de l'utilisateur qui doit exécuter une commande directement après le tableau des horaires. Dans l'exemple 10.1 page ci-contre, l'utilisateur `root` est entré. Des tableaux se rattachant à un paquetage en particulier ont le même format et se trouvent dans le répertoire `/etc/cron.d`.

Example 10.1: *Exemple de déclaration dans /etc/crontab*

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Le fichier `/etc/crontab` ne peut pas être édité à l'aide de la commande `crontab -e` mais il doit être chargé directement dans un éditeur pour y recevoir les modifications prévues et y être enregistré.

Un certain nombre de paquetages installent dans les répertoires `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` et `/etc/cron.monthly` des scripts shell dont les instructions sont gérées par `/usr/lib/cron/run-crons`. Toutes les quinze minutes, la table principale (`/etc/crontab`) appelle `/usr/lib/cron/run-crons`, ce qui permet de rattraper éventuellement les étapes qui n'ont pas pu être traitées à temps.

Pour plus de clarté, les travaux de maintenance exécutés quotidiennement sur le système sont répartis sur plusieurs scripts. Ils sont contenus dans le paquetage `aaa_base`. Ainsi, le répertoire `/etc/cron.daily` comporte, par exemple, les composants `backup-rpmdb`, `clean-tmp` ou `clean-vi`.

10.1.3 Fichiers journaux — le paquetage logrotate

De nombreux services système ("démons") ainsi que le noyau lui-même enregistrent régulièrement l'état du système et d'éventuels incidents dans des fichiers journaux (logfiles). L'administrateur peut ainsi déterminer de façon fiable dans quel état le système se trouvait à un instant donné, identifier les erreurs ou les dysfonctionnements et réagir de façon appropriée. Ces fichiers journaux se trouvent, conformément au standard FHS, dans le répertoire `/var/log` et grossissent de jour en jour. On peut contrôler la croissance de ces fichiers à l'aide de `logrotate`.

Configuration

Le fichier de configuration `/etc/logrotate.conf` définit le comportement d'ensemble. La directive `include` permet de nommer les fichiers supplémentaires devant être chargés. Il est prévu que les différents paquetages de SUSE LINUX installent des fichiers dans `/etc/logrotate.d`. (par exemple `syslog` et YaST procèdent ainsi).

Example 10.2: Exemple de fichier /etc/logrotate.conf

```
# see "man logrotate" for details
# rotate log files weekly weekly
# keep 4 weeks worth of backlogs rotate 4
# create new (empty) log files after rotating old ones create
# uncomment this if you want your log files compressed
#compress
# RPM packages drop log rotation information into this directory
include /etc/logrotate.d
# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}
# system-specific logs may be also be configured here.
```

logrotate lui-même est contrôlé par cron et déclenché quotidiennement par `/etc/cron.daily/logrotate`.

Important

L'option `create` lit les préférences éventuelles de l'administrateur dans les fichiers `/etc/permissions*`. Assurez-vous que cela n'entre pas en conflit avec vos réglages.

Important

10.1.4 Les pages de manuel

Pour un certain nombre de programmes GNU (par exemple tar), les pages de manuel ne sont plus tenues à jour. Utilisez alors l'option `--help` pour obtenir une présentation rapide ou les page d'info. Le programme info constitue le système hypertexte du système GNU. La commande `info info` donne accès à une première aide à l'utilisation. Les pages info peuvent être vues dans Emacs en exécutant `emacs -f info` ou bien directement dans une console à l'aide de la commande `info`. Vous pouvez également utiliser les applications tkinfo, xinfo ou le système d'aide SUSE pour visualiser les pages info.

10.1.5 La commande locate

locate, qui permet de trouver rapidement des fichiers, ne fait pas partie des logiciels installés par défaut. Installez-le (`find-locate`) si vous souhaitez l'utiliser. Le processus updatedb sera alors démarré quotidiennement de façon automatique, la nuit ou environ 15 minutes après l'amorçage du système.

10.1.6 La commande ulimit

La commande `ulimit` (*user limits*) permet de fixer des limites à l'utilisation des ressources système et d'afficher ces dernières. `ulimit` est utilisé notamment pour limiter la mémoire allouée aux applications. Ainsi, on peut éviter qu'une application ne monopolise la majeure partie ou la totalité de la mémoire et ne gèle le système.

Le programme `ulimit` peut être exécuté avec différentes options. Pour restreindre l'utilisation de la mémoire, utilisez les options affichées dans le tableau 10.1 de la présente page.

TAB. *10.1:* *ulimit : configuration des ressources de l'utilisateur*

`-m`	taille maximale de la mémoire physique
`-v`	taille maximale de la mémoire virtuelle
`-s`	taille maximale de la pile
`-c`	taille maximale des fichiers Core (de vidage mémoire)
`-a`	affichage des limites fixées

La configuration pour tout le système peut être définie dans le fichier `/etc/profile`. Activez-y la création de fichiers core dont les programmeurs ont besoin pour le "débogage". Les utilisateurs normaux ne sont pas autorisés à augmenter les valeurs fixées par l'administrateur système dans `/etc/profile`. Ils peuvent toutefois saisir des paramètres particuliers dans leur propre fichier `~/.bashrc`.

Example 10.3: *Paramètres ulimit dans ~/.bashrc*

```
# Limitation de la mémoire réelle
ulimit -m 98304

# Limitation de la mémoire virtuelle
ulimit -v 98304
```

La mémoire doit être exprimée en Ko. Pour plus de précisions, reportez-vous à la page de manuel `man bash`.

Important

Tous les interpréteurs de commandes (shells) ne prennent pas en charge les directives `ulimit`. Dans le cas où vous auriez besoin de définir des paramètres globaux fixant ces limitations, vous pouvez utiliser PAM (par exemple `pam_limits`) qui offre des possibilités de configuration avancées.

Important

10.1.7 La commande free

La commande `free` prête quelque peu à confusion lorsqu'il s'agit de déterminer comment la mémoire vive est utilisée à un moment donné. On trouve les informations correspondantes `/proc/meminfo`. De nos jours, cela ne devrait préoccuper aucun utilisateur d'un système d'exploitation moderne comme Linux. Le concept de *mémoire vive disponible* remonte à l'époque où la gestion unifiée de la mémoire (unified memory management) n'existait pas encore. Le slogan *La mémoire disponible est de la mauvaise mémoire* (free memory is bad memory) s'applique bien à Linux. En conséquence, Linux s'est toujours efforcé de trouver un équilibre entre les caches sans jamais accepter la présence de mémoire réellement libre ou inutilisée.

Le noyau n'a aucune idée des programmes ou des données utilisateurs. Il gère les programmes et les données utilisateurs dans la *mémoire cache*. Lorsque la mémoire commence à être saturée, une partie est écrite dans la partition d'échange (swap) ou dans des fichiers à partir desquels elle peut être initialement lue à l'aide de la commande `mmap` (voir `mmap`).

À côté de cela, le noyau utilise également d'autres zones de caches, comme le *slab cache*, qui contient les caches utilisés pour l'accès réseau. C'est ce qui permet d'expliquer d'éventuelles différences entre les valeurs dans `/proc/meminfo`. On peut accéder à pratiquement tous ces caches via `/proc/slabinfo`.

10.1.8 Le fichier /etc/resolv.conf

La résolution de noms est gérée par l'intermédiaire du fichier `/etc/resolv.conf`. Voyez le chapitre 24 page 463.

Ce fichier est actualisé par le script `/sbin/modify_resolvconf` exclusivement. Aucun autre programme n'est autorisé à manipuler directement le fichier `/etc/resolv.conf`. Cette règle doit être respectée pour assurer la cohérence entre la configuration réseau et les fichiers appropriés.

10.1.9 Configuration de GNU Emacs

GNU Emacs est un environnement complexe. Pour de plus amples informations, consultez `http://www.gnu.org/software/emacs/`. Dans les sections suivantes, nous passerons en revue les fichiers de configuration sur lesquels GNU Emacs se base au démarrage.

Au démarrage, Emacs lit plusieurs fichiers contenant les réglages de l'utilisateur, de l'administrateur système et du distributeur pour s'adapter et se préconfigurer en fonction de leurs besoins respectifs. Le fichier d'initialisation `~/.emacs` est installé, pour chaque utilisateur, à partir de `/etc/skel` dans le répertoire personnel. Le fichier `.emacs` charge à son tour le fichier `/etc/skel/.gnu-emacs`. Pour personnaliser le programme, copiez le fichier `.gnu-emacs` dans le répertoire personnel (avec `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`), puis procédez aux réglages souhaités.

Dans `.gnu-emacs`, le fichier `~/.gnu-emacs-custom` est répertorié comme `custom-file`. Si les utilisateurs définissent des paramètres avec les options `customize`, ces modifications seront enregistrées dans `~/.gnu-emacs-custom`.

Sous SUSE LINUX, avec le paquetage `emacs`, le fichier `site-start.el` est installé dans le répertoire `/usr/share/emacs/site-lisp`. Le fichier `site-start.el` est chargé avant le fichier d'initialisation `~/.emacs`. Le fichier `site-start.el` permet entre autres de charger certains fichiers de configuration installés avec des paquetages Emacs additionnels de la distribution (par exemple le paquetage `psgml`). De tels fichiers de configuration se trouvent également dans le répertoire`/usr/share/emacs/site-lisp` et commencent toujours par `suse-start-`. L'administrateur système local peut enregistrer des réglages s'appliquant à tout le système dans le fichier `default.el`.

Pour plus d'informations, consultez le fichier info d'Emacs sous *Init File* : `info:/emacs/InitFile`. Il y est notamment décrit comment empêcher le chargement de ces fichiers (si besoin est).

Les composants d'Emacs sont répartis dans plusieurs paquetages :

- Paquetage de base `emacs`
- Paquetage `emacs-x11` (généralement installé) : programme *avec* prise en charge de X11.
- Paquetage `emacs-nox` programme *sans* prise en charge de X11.
- Paquetage `emacs-info` : documentation en ligne au format Info.
- Paquetage `emacs-el` : fichiers de bibliothèque non compilés en Lisp Emacs. Ceux-ci ne sont pas nécessaires à l'exécution.
- De nombreux paquetages supplémentaires peuvent être installés si besoin est : le paquetage `emacs-auctex` (pour LaTeX) ; le paquetage `psgml` (pour SGML/XML) ; le paquetage `gnuserv` (pour l'utilisation en modes client et serveur), etc.

10.1.10 Brève initiation au vi

Pour beaucoup de travaux sur le système, mais également pour des travaux de programmation, on utilise encore aujourd'hui des éditeurs de texte. Dans le domaine Unix, le vi s'est au fil du temps imposé comme étant l'éditeur qui offre de fonctions confortables d'édition et est beaucoup plus ergonomique que beaucoup d'éditeurs prenant également en charge la souris.

Modes de fonctionnement

On différencie en principe dans l'éditeur vi trois différents modes de fonctionnement : le mode *insertion*, le mode *commande* et le mode *étendu*. Les touches ont des fonctions très différentes selon le mode. La première chose à savoir est comment commuter entre les modes :

Du mode commande vers le mode insertion
Il existe ici une grand nombre de possibilités, dont : (A) pour ajouter, (I) pour insérer ou (O) pour une nouvelle ligne sous la ligne actuelle.

Du mode insertion vers le mode commande
Pour quitter le mode *insertion*, pressez la touche (Esc). Dans le mode *insertion*, il n'est pas possible de quitter l'éditeur vi. C'est pourquoi il est important de garder la touche (ESC) en mémoire.

Du mode commande vers le mode étendu
Le mode *étendu* de l'éditeur vi peut être activé en saisissant deux-points ((:)). Le mode *étendu*, appelé aussi mode *ex*, correspond à un éditeur indépendant fonctionnant ligne par ligne. Vous pouvez, à l'aide de ce mode, effectuer de nombreuses tâches, des plus simples au plus complexes.

Du mode étendu vers le mode commande

Après l'exécution d'une commande dans le mode *étendu*, on revient en principe automatiquement dans le mode *commande*. Cependant, si vous décidez finalement de n'exécuter aucune commande en mode *étendu*, vous pouvez, à l'aide de la touche de ⟵, effacer les deux-points. L'éditeur repasse alors en mode *commande*.

Notez qu'une commutation du mode *insertion* vers le mode *étendu* nécessite toujours le passage intermédiaire par le mode *commande*. Une commutation directe n'est pas possible.

vi, comme d'autres éditeurs, possède sa propre procédure pour quitter le programme. Il est impossible de quitter vi en mode *insertion*. Quittez d'abord le mode *insertion* avec la touche Esc. Puis, on différencie deux cas de figure :

1. *Quitter sans enregistrer :* si vous désirez quitter l'éditeur sans enregistrer les modifications, saisissez, dans le mode *commande*, la combinaison de touches : Q !. ! signifie à vi d'ignorer les modifications effectuées.
2. *Quitter et enregistrer :* pour enregistrer les modifications et ensuite quitter l'éditeur, vous disposez de plusieurs possibilités. Dans le mode *commande*, utilisez Shift Z Z. Dans le mode *étendu*, utilisez : W Q. Dans le mode *étendu*, W signifie "write" (écrire) et Q signifie "quit" (quitter).

vi en pratique

vi peut être utilisé comme un éditeur tout à fait normal. Dès que vous êtes en mode *insertion*, vous pouvez entrer du texte et en effacer à l'aide des touches de retour en arrière ⟵ et d'effacement et Suppr. Pour bouger le curseur, utilisez les touches de contrôle du curseur.

Mais on est souvent confronté à des problèmes, justement avec ces touches de commande. Ceci provient du fait qu'il existe un grand nombre de types de terminaux différents qui utilisent chacun des codes de touches qui leur sont propres. C'est à ce moment qu'entre en jeu le mode *commande*. Appuyez sur la touche Esc pour passer du mode *insertion* en mode *commande*. Dans le mode *commande*, déplacez le curseur avec les touches H, J, K et L. Ces touches ont les significations suivantes :

H déplace le curseur d'un caractère vers la gauche

J déplace le curseur d'une ligne vers le bas

K déplace le curseur d'une ligne vers le haut

L déplace le curseur d'un caractère vers la droite

Les commandes en mode *commande* permettent diverses variations. Si vous désirez exécuter plusieurs fois une commande, vous pouvez entrer simplement sous forme de chiffre le nombre de répétitions, et ensuite appeler la commande voulue. Donc, si vous entrez la séquence de commande 5 L, le curseur bougera de cinq caractères vers la droite.

Informations complémentaires

L'éditeur vi prend en charge énormément de commandes. ll permet l'utilisation de macros, de raccourcis, de tampons et beaucoup d'autres fonctionnalités. Les décrire ici en détails nous mènerait trop loin. SUSE LINUX contient une version améliorée de vi, le vim (vi improved). Il existe de nombreuses sources d'informations traitant de ce programme :

- vimtutor est un didacticiel interactif pour vim.
- Dans vim, saisissez la commande `:help` pour obtenir de l'aide sur de nombreux sujets.
- Un livre en ligne sur vim (en anglais) est disponible à l'adresse `http://www.truth.sk/vim/vimbook-OPL.pdf`.
- Sur les pages web du projet vim, vous trouverez toutes les nouveautés, les listes de diffusion et autres documentations. Vous trouverez ces pages à l'adresse `http://www.vim.org`.
- Vous trouverez sur internet également de nombreuses sources d'informations au sujet de vim : `http://www.selflinux.org/selflinux/html/vim.html`, `http://www.linuxgazette.com/node/view/9039` et `http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html`. Vous trouverez d'autres liens vers des didacticiels sous `http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html`.

Important

La licence VIM

vim est ce qu'on appelle un "logiciel de bienfaisance". Ceci signifie que les auteurs ne veulent pas recevoir d'argent pour les logiciels mais qu'ils incitent à supporter un projet d'intérêt général à l'aide de dons. Ce projet servira à venir en aide aux enfants en Ouganda. Vous trouverez de plus amples informations à ce sujet sur internet sous `http://iccf-holland.org/index.html`, `http://www.vim.org/iccf/` et `http://www.iccf.nl/`.

Important

10.2 Consoles virtuelles

Linux est un système multitâches et multi-utilisateurs. Même si vous êtes le seul utilisateur sur votre machine, vous apprendrez à apprécier les avantages apportés par ces capacités. Vous avez accès à six consoles virtuelles en mode texte que vous pouvez activer à l'aide des combinaisons de touches Alt-F1 à Alt-F6. La septième console est réservée à X. En modifiant le fichier `/etc/inittab`, vous pouvez réserver plus ou moins de consoles.

Pour passer à une console texte depuis X sans avoir à l'arrêter, utilisez les combinaisons de touches Ctrl-Alt-F1 à Ctrl-Alt-F6. Alt-F7 vous permet de revenir à X.

10.3 Disposition du clavier

Les fichiers suivants ont été modifiés afin d´uniformiser la disposition du clavier pour les programmes :

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
```

```
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/<VERSION>/site-lisp/term/*.el
```

Ces modifications n'affectent que les applications qui utilisent les entrées de `terminfo` ou dont les fichiers de configuration ont été modifiés directement (`vi`, `less`, etc.). Il est conseillé d'adapter sur ce modèle les applications qui ne sont pas livrées avec SUSE LINUX.

Vous obtiendrez la touche compose (multikey) sous X grâce à la combinaison de touches Ctrl-Shift (droite). Voyez aussi l'entrée correspondante dans `/usr/X11R6/lib/X11/Xmodmap`.

L'"extension X Keyboard" (XKB) permet une configuration plus poussée. Cette extension est utilisée également par les environnements de bureau GNOME (gswitchit) et KDE (kxkb). Vous trouverez plus d'informations relatives à XKB dans `/etc/X11/xkb/README` et les documents qui y sont cités.

Vous trouverez des informations supplémentaires concernant la saisie en chinois, japonais ou coréen (CJC) sur le site de Mike Fabian : `http://www.suse.de/~mfabian/suse-cjk/input.html`.

10.4 Adaptations régionales et linguistiques

SUSE LINUX est très largement internationalisé et s'adapte avec souplesse aux contraintes locales. L'internationalisation (*I18N*) permet des localisations dans des langues particulières (*L10N*). Les abréviations I18N et L10N signifient respectivement *internationalisation* et *localisation* : on prend l'initiale et la dernière lettre et on fait figurer entre elles le nombre de lettres omises.

Les réglages se font au moyen des variables `LC_` définies dans le fichier `/etc/sysconfig/language`. Il ne s'agit pas seulement de régler la *prise en charge globale de la langue*, mais de régler individuellement les catégories suivantes : les *messages* (langue), les *jeux de caractères*, l'*ordre de classement*, les *date et heure*, les *nombres* et la *monnaie*. Chacune de ces catégories peut être définie soit de manière ciblée grâce à une variable propre soit indirectement grâce à une variable principale dans le fichier `language` (voir la page de manuel `man locale`).

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`

Ces variables sont passées à l'interpréteur de commandes sans le préfixe

RC_ et définissent les catégories nommées plus haut. Les fichiers concernés sont énumérés ci-après. Vous pouvez afficher le réglage courant grâce à la commande `locale`.

RC_LC_ALL Cette variable écrase, si elle a été initialisée, les valeurs des variables de la liste.

RC_LANG Si aucune des variables nommées plus haut n'a été initialisée, on se rabat sur cette valeur. Par défaut, SUSE LINUX ne définit que `RC_LANG` ; ainsi, il est plus simple pour l'utilisateur de saisir ses propres valeurs.

ROOT_USES_LANG Une variable binaire `yes` ou `no`. Si elle vaut `no`, `root` travaille toujours dans l'environnement POSIX.

Les variables peuvent être réglées grâce à l'éditeur sysconfig de YaST. La valeur d'une telle variable est composée de l'indication du code de la langue (language code), du pays ou du territoire (country code), de l'encodade des caractères (encoding) et du modificateur (modifier). Les différentes indications sont séparées par des caractères spéciaux :

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

10.4.1 Quelques exemples

Il est important de toujours définir conjointement la langue et le pays. Le code de langue suit le standard ISO 639 (`http://www.evertype.com/standards/iso639/iso639-en.html` et `http://www.loc.gov/standards/iso639-2/`). Les codes de pays sont définis dans la norme ISO 3166 (voir `http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html`). Naturellement, il ne faut choisir que des valeurs pour lesquelles il existe des fichiers de description utilisables dans `/usr/lib/locale`. On peut générer de nouveaux fichiers de description à l'aide de `localedef` sur la base des fichiers contenus dans `/usr/share/i18n` ; les fichiers de description font partie du paquetage `glibc-i18ndata`. On peut créer un fichier de description pour `fr_FR.UTF-8` (pour le français et la France) avec :

```
localedef -i fr_FR -f UTF-8 fr_FR.UTF-8
```

LANG=fr_FR.UTF-8 Il s'agit de la configuration par défaut lorsque l'on effectue l'installation en français. Si une autre langue est sélectionnée pour l'installation, l'encodage des caractères restera UTF-8, mais la langue du système sera celle de l'installation.

LANG=fr_FR.ISO-8859-1 C'est avec cette commande qu'on associe à la langue française le jeu de caractères ISO-8859-1. Ce jeu de caractères ne comprend pas le caractère euro. On l'utilise toutefois lorsqu'un logiciel n'a pas été adapté pour prendre en charge l'encodage UTF-8. La chaîne qui définit le jeu de caractère (ISO-8859-1 dans ce cas) est alors évaluée par des programmes tels que Emacs.

LANG=fr_FR@euro Cet exemple inclut explicitement le signe euro. À strictement parler, cette sélection est maintenant inutile car UTF-8 prend également en compte le symbole euro. Elle se révèle utile uniquement lorsque votre application ne prend pas en charge UTF-8 mais ISO-8859-15.

SuSEconfig lit les variables de `/etc/sysconfig/language` et écrit les changement nécessaires dans `/etc/SuSEconfig/profile` et `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` est lu par `/etc/profile` et `/etc/SuSEconfig/csh.cshrc` par `/etc/csh.cshrc`. De cette manière, les réglages sont disponibles pour tout le système.

Les utilisateurs peuvent écraser les réglages par défaut du système dans `~/.bashrc`. Donc, dans le cas où le réglage global est `fr_FR`, l'utilisateur peut, en incluant `LC_MESSAGES=es_ES` obtenir tout de même les messages des programmes en anglais.

10.4.2 Paramètres pour la prise en charge de la langue

Les fichiers de la catégorie *Messages* se trouvent en général uniquement dans le répertoire propre à la langue (par exemple `fr`), afin d'avoir une solution de repli. Donc, si l'on règle `LANG` sur `fr_CA` alors que le fichier *message* n'existe pas dans `/usr/share/locale/fr_CA/LC_MESSAGES`, les programmes se rabattent sur `/usr/share/locale/fr/LC_MESSAGES`.

On peut également définir une chaîne de replis successifs par exemple : de breton vers français ou de galicien vers espagnol puis vers portugais :

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

On peut également utiliser les variantes norvégiennes *nynorsk* et *bokmål* (avec un repli supplémentaire sur `no`) :

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

ou

```
LANG="nb_NO"
LANGUAGE="nb_NO:nn_NO:no"
```

Pour ce qui est du norvégien, il faut également tenir compte du fait que `LC_TIME` est traité différemment.

Le point marquant les milliers n'est pas reconnu : `LANG` est probablement réglé par exemple sur `fr`. Comme la description à laquelle la bibliothèque glibc fait appel se trouve dans `/usr/share/lib/fr_FR/LC_NUMERIC`, `LC_NUMERIC` devrait valoir par exemple `fr_FR`.

10.4.3 Informations complémentaires

- *The GNU C Library Reference Manual*, chapitre "Locales and Internationalization" ; contenu dans le paquetage `glibc-info`.
- *Howto francophones* de Guylhem-Aznar `file:/usr/share/doc/howto/en/html/Francophones-HOWTO.html`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, actuellement à l'adresse suivante : `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- *Howto Unicode* de Bruno Haible en anglais `file:/usr/share/doc/howto/en/html/Unicode-HOWTO.html` ou en français `file:/usr/share/doc/howto/fr/a-jour/html/Unicode-HOWTO.html`.

Le système X Window

Le système X Window (X11) est pratiquement le standard pour les interfaces utilisateur graphiques sous UNIX. X est orienté réseau : ainsi des applications exécutées sur un ordinateur peuvent afficher leurs résultats sur un autre ordinateur, lorsque ces deux ordinateurs sont connectés l'un à l'autre, quelque soit le type de réseau (réseau local LAN ou Internet).

Ce chapitre décrit la mise en place, les possibilités d'optimisation, des informations de base sur l'utilisation des polices de caractères sous SUSE LINUX et la configuration de OpenGL et 3D.

11.1 Configuration de X11 avec SaX2

L'interface graphique, ou serveur X, rend possible la communication entre le matériel et les logiciels. Les bureaux, comme KDE et GNOME et la majorité des gestionnaires de fenêtres, utilisent le serveur X pour l'interaction avec l'utilisateur.

L'interface graphique est configurée lors de l'installation. Si vous voulez modifier les paramètres de configuration par la suite, utilisez SaX2.

Les valeurs actuelles sont enregistrées et pourront être réinitialisées à tout moment. Elles sont affichées et proposées à la modification : la résolution de l'écran, la profondeur de couleurs, le taux de rafraîchissement et les fabricant et modèle du moniteur, si ces données ont été reconnues automatiquement.

Si vous venez d'installer une nouvelle carte graphique une petite fenêtre apparaît dans laquelle vous devrez préciser si vous voulez activer l'accélération 3D pour votre carte graphique. Cliquez sur 'Modifier'. Maintenant, SaX2, l'outil de configuration des périphériques d'entrée et d'affichage, démarre dans une fenêtre séparée représentée dans la figure 11.1 de la présente page.

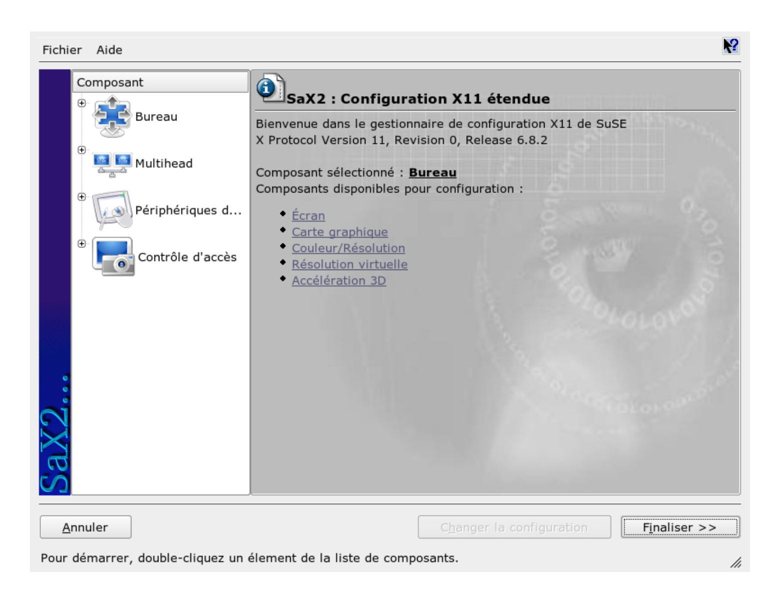


FIG. 11.1: *La fenêtre principale de SaX2*

Dans la barre de navigation à gauche se trouvent quatre options principales : 'Bureau', 'Périphériques d'entrée', 'Multihead' et 'AccessX'. Dans 'Bureau', vous pouvez configurer le moniteur, la carte graphique, la profondeur de couleurs et la résolution ainsi que la taille et la position de l'image. Dans 'Périphériques d'entrée' vous pouvez configurer le clavier et la souris ainsi que, si nécessaire, un écran tactile et une tablette graphique. Dans le menu 'Multihead', vous pouvez configurer une station avec écrans multiples (voir la section 11.1.7 page 240). 'AccessX' est un outil très pratique pour contrôler le pointeur de la souris avec les touches du pavé numérique du clavier.

Entrez le modèle approprié pour le moniteur et la carte graphique. En général, le système reconnaît automatiquement l'écran et la carte graphique. Si votre système ne reconnaît pas votre moniteur, le dialogue de selection de moniteurs apparaît avec une liste de fabricants et modèles, dans laquelle vous trouverez très probablement le votre. Si ce n'est pas le cas, entrez manuellement les valeurs qui correspondent à votre moniteur ou choisissez l'un des modes Vesa préconfigurés.

Cliquez, dans la fenêtre principale, sur 'Terminer' une fois que la configuration du moniteur et de la carte graphique est achevée puis procédez à un test de la configuration. De cette façon, vous pouvez vous assurer que la configuration choisie fonctionne sans problème. Si l'image qui est affichée est trouble, interrompez le test immédiatement en pressant la touche Esc et réduisez la valeur du taux de rafraîchissement de l'image ou la résolution et la profondeur de couleurs. Toutes les modifications réalisées, que vous les ayez testées ou non, sont activées lors du redémarrage du serveur X.

11.1.1 Bureau

Sélectionnez 'Modifier la configuration' → 'Propriétés', une fenêtre contenant les trois onglets'Moniteur', 'Fréquences' et 'Avancé' apparaît.

'Moniteur' Sélectionnez ici le fabricant dans la partie gauche de la fenêtre et le modèle dans la partie droite. Si vous avez une disquette de pilotes Linux pour votre moniteur, utilisez-la après avoir cliqué sur 'Disquette de pilotes'.

'Fréquences' Entrez ici les fréquences horizontales et verticales appropriées pour votre moniteur. La fréquence verticale est une autre dénomination pour le taux de rafraîchissement de l'image. Normalement, ces valeurs sont déterminées automatiquement en fonction du modèle de moniteur et vous n'avez besoin de procéder à aucun changement.

'Avancé' Vous pouvez ici configurer quelques options pour votre moniteur. Dans le champ de saisie, vous pouvez spécifier la méthode à utiliser pour

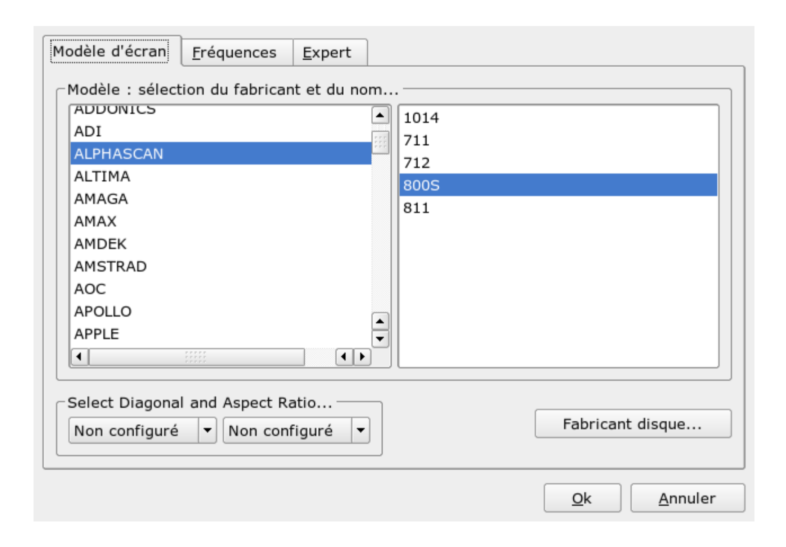


FIG. *11.2: Sélection du moniteur*

le calcul de la résolution et de la géométrie de l'écran. Ne procédez ici à des modifications que dans le cas où votre écran a posé des problèmes. En outre, vous pouvez changer la taille de l'image affichée et activer le mode de gestion d'énergie DPMS que vous souhaitez.

Avertissement

Configuration des fréquences du moniteur

Malgré les mécanismes de protection implémentés, soyez prudent lors de la modification manuelle des fréquences. Des valeurs erronées peuvent endommager votre moniteur. En cas de doute, consultez le manuel accompagnant votre moniteur.

Avertissement

11.1.2 Carte graphique

Dans le dialogue de la carte graphique, vous verrez deux onglets : 'Général' et 'Avancé'. Dans l'onglet 'Général', sélectionnez le fabricant à gauche et le modèle de carte graphique à droite.

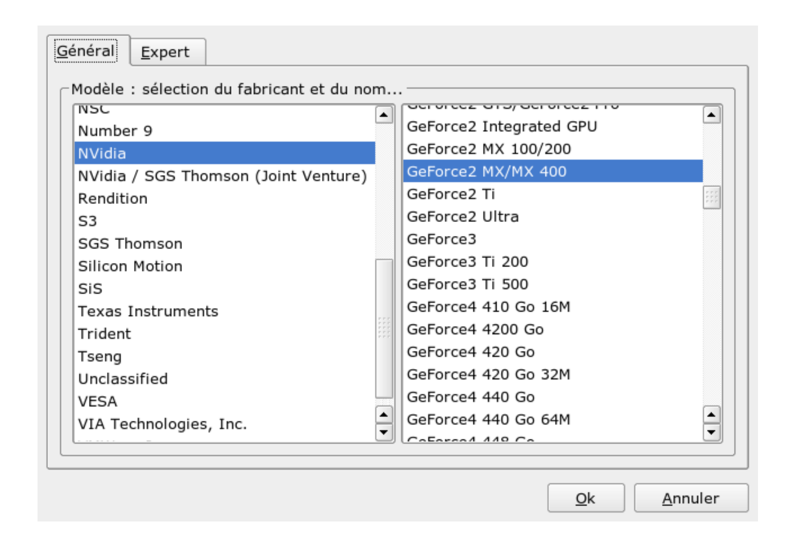


FIG. 11.3: *Sélection de la carte graphique*

'Avancé' offre plus d'options de configuration avancées. À droite, spécifiez si vous voulez orienter votre écran verticalement ou horizontalement (ceci ne concerne que certains écrans TFT orientables). Les entrées pour le BusID ne présentent d'intérêt que si vous travaillez avec plus d'un écran. En général, vous n'avez rien à changer ici. Surtout, ne procédez à aucune modification si vous ne connaissez pas la signification des différentes options. Si nécessaire, consultez la documentation qui accompagne votre carte graphique pour connaître la signification des différentes options.

11.1.3 Couleurs et résolutions

Ici, vous trouverez les trois onglets 'Couleurs', 'Résolution' et 'Avancé'.

'Couleurs' Selon le matériel utilisé, vous pouvez choisir une profondeur de couleurs de 16, 256, 32768, 65536 et 16,7 millions de couleurs (4, 8, 15, 16 ou 24 bits). Pour une qualité d'affichage raisonnable, sélectionnez au moins 256 couleurs.

'Résolution' Toutes les combinaisons de résolution et profondeur de couleurs supportées sans problème par votre matériel vous sont proposées. Ainsi le

danger d'endommager votre matériel en utilisant de mauvais paramètres est très réduit avec SUSE LINUX. Si vous souhaitez tout de même modifier manuellement les valeurs de résolution, consultez absolument la documentation de votre matériel pour savoir si les valeurs que vous souhaitez utiliser ne poseront pas de problème.

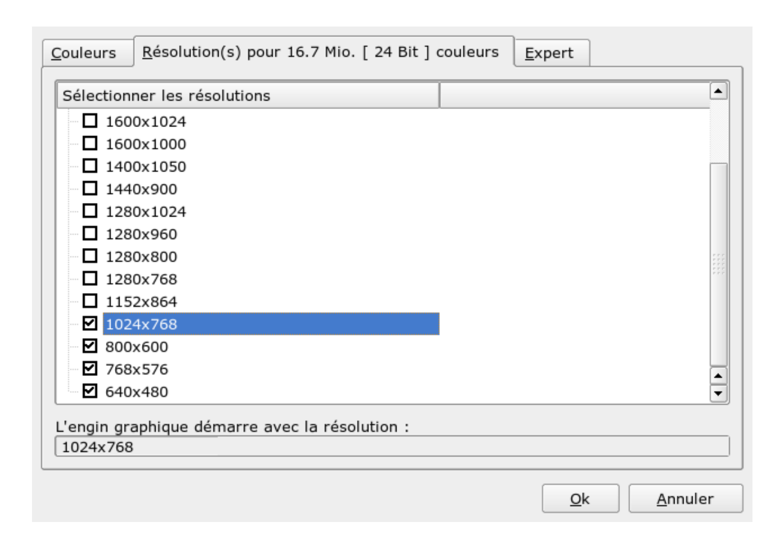


FIG. 11.4: *Configuration de la résolution*

'Avancé' Ici, vous pouvez ajouter des résolutions à celles offertes dans l'onglet précédent. Celles-ci seront alors ajoutées à la sélection.

11.1.4 Résolution virtuelle

Chaque interface possède une résolution propre, visible sur tout l'écran. Outre cette résolution, vous pouvez configurer une autre résolution plus importante que la zone visible de l'écran. Si vous sortez de l'écran avec le curseur de la souris, vous déplacerez la zone virtuelle dans la zone visible. La taille des pixels ne change pas, mais la surface d'utilisation est plus grande. C'est ce que l'on appelle la résolution virtuelle.

La configuration de la résolution virtuelle peut se faire de deux façons. 'Par glissé-déposé', déplacez la souris dans la zone visible de l'écran, le pointeur de la souris se convertit en un réticule. Cliquez sur le bouton de gauche de la souris

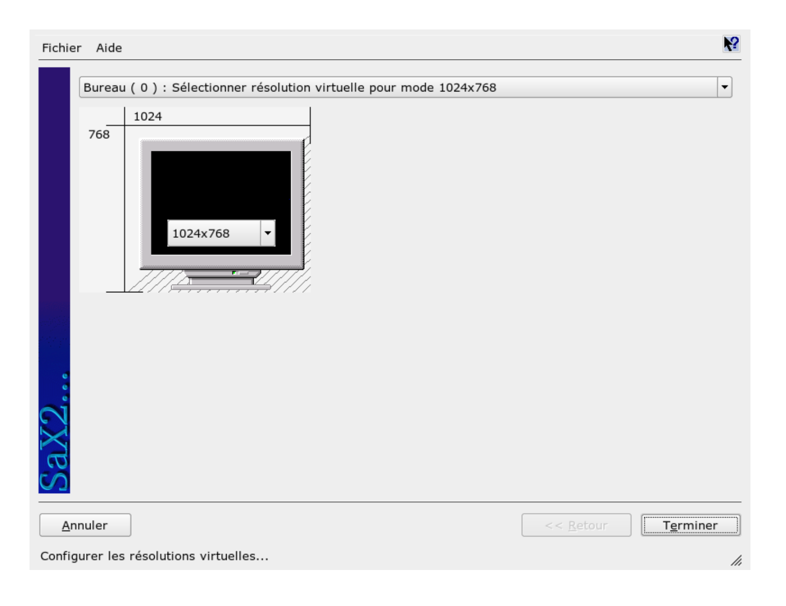


FIG. 11.5: *Configuration de la résolution virtuelle*

et maintenez-le enfoncé pendant que vous déplacez la souris, vous modifiez ainsi la taille de la surface marquée. Cette surface affiche la résolution virtuelle correspondant à la résolution réelle représentée sur l'écran. Cette méthode de configuration est conseillée lorsque vous ne souhaitez employer comme zone virtuelle qu'une zone déterminée dont vous ne connaissez pas encore exactement la taille.

Avec 'À l'aide d'une sélection dans le menu déroulant', le menu déroulant qui se trouve au milieu de la surface marquée affiche la résolution virtuelle configurée actuellement. Pour utiliser l'une des résolutions virtuelles par défaut, sélectionnez-en une dans le menu.

11.1.5 Accélération 3D

Si pendant l'installation initiale ou lors de la connexion d'une nouvelle carte graphique et de sa configuration, vous n'avez pas activé l'accélération 3D, vous pouvez le faire ici.

11.1.6 Taille et position de l'image

Dans ces deux onglets, vous pouvez, à l'aide des flèches, ajuster précisément la taille et la position de l'image. Voir la figure 11.6 de la présente page). Si vous travaillez dans un environnement multihead (plus d'un écran), vous pouvez passer sur les autres moniteurs à l'aide du bouton 'Écran suivant' pour fixer leur taille et position. Avec 'Enregistrer', vous enregistrez votre configuration.

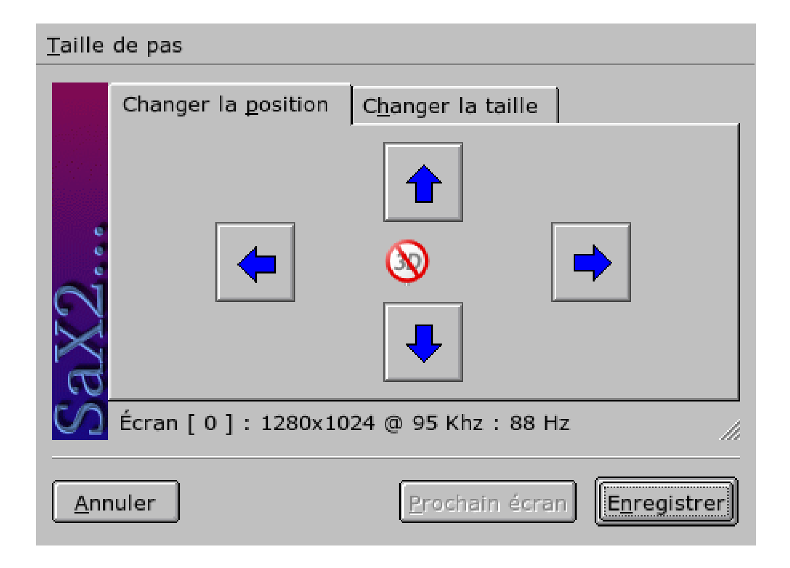
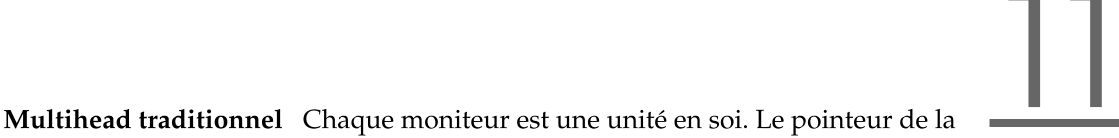


FIG. *11.6: Ajustement de la géométrie de l'image*

11.1.7 Multihead

Si votre ordinateur est équipé de plus d'une carte graphique ou d'une carte graphique à plusieurs sorties, vous pourrez travailler avec plus d'un écran. Si vous utilisez deux écrans, il s'agit de *dualhead*, si vous travaillez avec plus de deux écrans, il s'agit de *multihead*. SaX2 détermine automatiquement les cartes graphiques multiples dans votre système et prépare la configuration appropriée. Dans le dialogue multihead, spécifiez le mode multihead et la disposition des écrans. Vous pouvez choisir entre trois modes : 'Traditionnel' (par défaut), 'Xinerama' et 'Cloné'.



Multihead traditionnel Chaque moniteur est une unité en soi. Le pointeur de la souris peut passer d'un écran à un autre.

Multihead cloné Ce mode est utilisé lors de présentations et salons lorsque tout un mur d'écrans est installé. Dans ce mode, tous les moniteurs ont le même contenu. La souris n'apparaît que dans l'écran principal.

Multihead Xinerama Tous les écrans fusionnent en un seul grand écran. Les fenêtres des programmes peuvent être placés sur tous les moniteurs ou avoir une taille supérieure à celle d'un écran.

La disposition d'un environnement multihead décrit la distribution et les relations de comportement entre les différents écrans. Par défaut, SaX2 réalise une disposition en ligne de gauche à droite selon l'ordre des cartes graphiques reconnues. Dans le dialogue 'Disposition' de l'outil multihead, vous pouvez déterminer la disposition de vos moniteurs. Pour cela, il vous suffit de déplacer dans la grille les symboles des écrans avec la souris et de les ordonner comme vous le souhaitez. Après avoir fermé le dialogue de disposition, vous pouvez tester la nouvelle configuration en cliquant sur le bouton 'Test'.

Veuillez noter que, pour le moment, Linux n'offre pas l'accélération 3D pour un environnement multihead Xinerama. Dans ce cas, SaX2 désactivera le support 3D.

11.1.8 Périphériques d'entrée

Souris Si le processus de reconnaissance automatique ne reconnaît pas la souris, vous devrez configurer votre souris manuellement. Vous pouvez trouver le type de la souris dans sa documentation. Choisissez la valeur correspondante dans la liste de modèles des souris supportées. Après avoir marqué le modèle adéquat, confirmez la sélection en pressant la touche ⑤ du pavé numérique.

Clavier Dans le champ de sélection de ce dialogue, vous pouvez déterminer le type de clavier que vous utilisez. En-dessous, vous pouvez choisir la langue pour la disposition du clavier (la position des touches spécifique au pays). Finalement, vous pouvez vérifier si cette disposition du clavier fonctionne en saisissant quelques caractères spéciaux dans le champ de test. Saisissez, par exemple, "à", "ç", "ù" ou "ô".

L'état de la case à cocher qui vous permet d'activer ou de désactiver l'entrée de lettres accentuées dépend de la langue sélectionnée et ne devrait pas être changé. Cliquez sur 'Terminer' pour appliquer les nouveaux paramètres de configuration à votre système.

Écran tactile À l'heure actuelle, uniquement les écrans tactiles des marques Microtouch et Elographics sont supportés par X.Org. SaX2 ne peut reconnaître que le moniteur automatiquement, mais pas le crayon (toucher). Le crayon peut être considéré comme un périphérique d'entrée.

Pour le configurer correctement, démarrez SaX2 et sélectionnez 'Périphériques d'entrée' → 'Écrans tactiles'. Cliquez sur 'Ajouter' et ajoutez un écran tactile. Enregistrez la configuration en cliquant sur 'Appliquer'. Il n'est pas nécessaire de tester la configuration.

Les écrans tactiles disposent d'une grande variété d'options et doivent généralement être qualibrés. Malheureusement, il n'existe pas d'outil global sous Linux pour cela. La configuration de la taille des écrans tactiles est déjà intégrée dans les valeurs par défaut de la configuration standard. Normalement, vous n'aurez pas à procéder à une configuration additionnelle.

Tablettes graphiques À l'heure actuelle, X.Org ne supportent que quelques tablettes graphiques. SaX2 permet la configuration des tablettes connectées au port USB comme au port série. Du point de vue de la configuration, une tablette graphique peut être considérée comme un périphérique d'entrée tel qu'une souris.

Démarrez SaX2 et sélectionnez 'Périphériques d'entrée' → 'Tablette graphique'. Cliquez sur 'Ajouter', sélectionnez le fabricant dans le dialogue suivant et choisissez une tablette graphique dans la liste. Utilisez les cases à cocher à droite pour spécifier si vous utilisez également un crayon et/ou une gomme. Dans le cas d'une tablette connectée à un port série, vérifiez si la connexion est correcte. `/dev/ttyS0` indique le premier port série, `/dev/ttyS1` le deuxième. Les ports supplémentaires utilisent une notation similaire. Enregistrez la configuration en cliquant sur 'Terminer'.

11.1.9 AccessX

Si vous travaillez sans souris, démarrez SaX2 et activez AccessX afin de pouvoir contrôler le pointeur de la souris à l'aide du pavé numérique de votre clavier. Voyez le tableau 11.1 page ci-contre pour une description des fonctions des différentes touches. Utilisez le curseur pour définir la vitesse de mouvement du pointeur de la souris lorsqu'une touche est pressée.

TAB. 11.1: *AccessX—contrôle de la souris à l'aide du pavé numérique*

Touche	Description
÷	Active le bouton de gauche de la souris
×	Active le bouton central de la souris
−	Active le bouton de droite de la souris
5	Cette touche vous permet de cliquer avec le bouton de la souris que vous avez activé auparavant. Si vous n'avez activé aucun bouton, c'est le bouton de gauche qui sera utilisé. Une fois que le clic aura été émulé, l'activation de la touche correspondante reviendra à sa configuration standard.
+	Cette touche fonctionne comme la touche 5, à la différence qu'elle émule un double-clic.
0	Cette touche fonctionne comme la touche 5, à la différence qu'elle émule une pression maintenue sur le bouton de la souris.
Supr	Cette touche émule le relâchement du bouton de souris maintenu enfoncé par l'action de la touche 0.
7	Déplace la souris vers le coin en haut à gauche
8	Déplace la souris en ligne droite vers le haut
9	Déplace la souris vers le coin en haut à droite
4	Déplace la souris vers la gauche
6	Déplace la souris vers la droite
1	Déplace la souris vers le coin en bas à gauche
2	Déplace la souris en ligne droite vers le bas
3	Déplace la souris vers le coin en bas à droite

11.1.10 Joystick

Avec ce module, vous pouvez configurer votre joystick en sélectionnant le fabricant et le modèle adéquats dans la liste affichée. Avec 'Test', vous pouvez vérifier si le joystick fonctionne correctement. Le dialogue de test affiche trois dia-

grammes à barres pour les axes analogiques du joystick et des marques pour les quatre boutons standards. Si vous bougez le joystick ou appuyez sur les boutons, la réaction correspondante doit apparaître dans le dialogue de test. Étant donné que la majorité des joysticks sont connectés à la carte son, vous pouvez également accéder à ce module depuis la configuration de la carte son.

11.2 Optimisation de la configuration X

Avec X.Org, vous disposez d'une implémentation Open Source du système X window. Celle-ci est développée par la fondation "X.Org Foundatation" qui est également responsable du développement de nouvelles technologies et standards du système X window.

Afin de pouvoir utiliser au mieux le matériel à votre disposition, souris, carte graphique, écran et clavier compris, vous pouvez optimiser la configuration manuellement. Nous présentons ici quelques aspects de l'optimisation. Vous trouverez des informations détaillées sur la configuration du système X window dans différents fichiers du répertoire `/usr/share/doc/packages/Xorg` ainsi, bien sûr, que dans la page de manuel `man xorg.conf`.

Avertissement

La configuration du système X window doit être réalisée avec un soin tout particulier ! Il ne faut en aucun cas démarrer le système X window avant d'avoir terminé la configuration. Un système mal configuré peut conduire à des dommages irréparables du matériel (les moniteurs à fréquence fixe sont à ce titre particulièrement menacés). Les auteurs de ce livre et la société SUSE LINUX AG déclinent toute responsabilité pour les dommages pouvant éventuellement survenir. Ce texte a été établi avec le plus grand soin. Nous ne pouvons cependant pas garantir que toutes les méthodes présentées ici sont correctes et ne causeront aucun dommage à votre matériel.

Avertissement

Par défaut, les programmes SaX2 et xf86config génèrent le fichier `xorg.conf` dans le répertoire `/etc/X11`. Ceci est le fichier de configuration primaire pour le système X window. C'est ici que se trouvent les données relatives à la souris, à l'écran et à la carte graphique.

La structure du fichier de configuration `/etc/X11/xorg.conf` vous est présentée ici. Ce fichier est partagé en sections introduites chacune par le mot-clé

`Section <description de la section>` et terminées par `EndSection`. Vous trouverez dans la suite une présentation sommaire des sections les plus importantes.

`xorg.conf` est composé de plusieurs sections qui traitent chacune d'un aspect de la configuration. Une section se présente toujours sous la forme :

```
Section description de la section
déclaration 1
déclaration 2
déclaration n
EndSection
```

Les types de sections disponibles sont répertoriés dans le tableau 11.2 de la présente page.

TAB. *11.2:* *Sections dans /etc/X11/xorg.conf*

Type	Signification
`Fichiers`	Cette section décrit les chemins utilisés pour les jeux de caractères et la palette chromatique RGB.
`ServerFlags`	Les commutateurs généraux sont renseignés ici.
`InputDevice`	Les périphériques d'entrée tels que les claviers et les souris aussi bien que les périphériques d'entrée spéciaux (tablettes graphiques, manettes de jeu, etc.) sont configurés dans cette section. Les identificateurs importants sont ici `Driver` et les options qui déterminent le protocole (`Protocol`) et le périphérique (`Device`).
`Monitor`	Décrit l'écran utilisé. Les éléments de cette section sont constitués d'un nom, auquel il est ensuite fait référence lors de la définition de l'affichage (`Screen`) ainsi que la description de la bande passante (`Bandwidth`) et des fréquences de synchronisation autorisées (`HorizSync` et `VertRefresh`). Les valeurs peuvent être indiquées en MHz, en kHz ou en Hz. Le serveur refuse en principe tout modeline ne correspondant pas aux spécifications de l'écran. Cela permet d'éviter d'envoyer par mégarde à l'écran des fréquences trop élevées.

`Modes`	C'est ici que sont fixés les paramètres représentatifs de chaque résolution d'écran. Ces paramètres peuvent être calculés par SaX2 sur la base des valeurs indiquées par l'utilisateur et, en règle générale, n'ont pas à être modifiés. Vous pouvez toutefois intervenir manuellement sur ces valeurs, par exemple si vous souhaitez intégrer un écran à fréquence fixe. Vous pouvez obtenir plus de précisions sur la signification des différentes valeurs des paramètres dans le fichier HOWTO `/usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz`.
`Device`	Cette section définit une carte graphique donnée. Celle-ci est référencée par la description.
`Screen`	Cette section lie un `Monitor` (écran) et un `Device` (carte graphique) pour former toutes les déclarations nécessaires pour X.Org. La sous-section `Display` permet de renseigner la taille de l'écran virtuel (`Virtual`), le `ViewPort` et les `Modes` utilisés avec cet écran.
`ServerLayout`	Cette section détermine la structure d'une configuration single ou multihead. Les périphériques d'entrée `InputDevice` et les périphériques d'affichage `Screen` sont liés dans cette section.

Les sections `Monitor`, `Device` et `Screen` sont abordées en détails. Vous trouverez plus d'information sur les autres sections dans la page de manuel de `X.Org` et dans la page de manuel de `xorg.conf`.

Dans `xorg.conf`, il peut exister plusieurs sections `Monitor` et `Device`. Plusieurs sections `Screen` sont également possibles ; c'est de la section suivante, `ServerLayout`, que va dépendre le choix de la section `Screen` utilisée.

11.2.1 Section Screen

La section Screen doit d'abord être considérée avec attention. Celle-ci comporte une section Monitor et une section Device et définit quelles résolutions doivent être mises à disposition avec quelle profondeur de couleurs. Une section Screen peut se présenter par exemple comme dans l'exemple 11.1 page ci-contre.

***Example 11.1:** La section Screen du fichier /etc/X11/xorg.conf*

```
Section "Screen"
  DefaultDepth  16
  SubSection "Display"
    Depth       16
    Modes       "1152x864" "1024x768" "800x600"
    Virtual     1152x864
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"
  Monitor       "Monitor[0]"
EndSection
```

La ligne `Identifier` (ici `Screen[0]`) donne à cette section un identificateur unique. On peut ensuite faire référence à cette section de manière univoque dans la section suivante `ServerLayout`. Les lignes `Device` et `Monitor` spécifient la carte graphique et l'écran qui appartiennent à cette définition. Ce ne sont donc rien de plus que des liens vers les sections de périphérique (`Device`) et d'écran (`Monitor`) au moyen des noms aussi appelés *identifiers* (identificateurs) correspondants. Ces sections sont décrites plus en détail ci-après.

Le paramètre `DefaultDepth` permet de définir la profondeur de couleurs avec laquelle le serveur démarre si aucune indication particulière ne lui est fournie au démarrage. Chaque profondeur de couleur est suivie d'une sous-section `Display`. La profondeur de couleurs valable pour la sous-section est fixée par le mot-clé `Depth`. Les valeurs possibles pour `Depth` sont 8, 15, 16 et 24. Tous les modules serveur X n'admettent pas forcément chacune de ces valeurs.

Après la profondeur de couleurs, on fixe une liste de résolutions dans la section `Modes`. Le serveur X parcourt cette liste de gauche à droite. Pour chaque résolution, il cherche une `Modeline` appropriée dans la section `Modes`. La modeline

dépend de la capacité d'affichage de l'écran et de la carte graphique à la fois. Les paramètres dans la section `Monitor` détermine la `Modeline` correspondante.

La première résolution appropriée, dans le sens où on l'entend ici, est celle avec laquelle démarre le serveur X (appelée `Default mode`). Avec les touches Ctrl-Alt-+ (sur le pavé numérique) on peut se déplacer dans la liste vers la droite, avec Ctrl-Alt-- (sur le pavé numérique) vers la gauche. On peut donc faire varier la profondeur de couleurs de l'écran pendant que X est en marche.

La dernière ligne de la sous-section `Display` avec `Depth 16` se rapporte à la taille de l'écran virtuel. La taille maximale possible de l'écran virtuel dépend de la quantité de mémoire installée sur la carte vidéo et de la profondeur de couleurs souhaitée, et non de la résolution maximale de l'écran. Comme les cartes graphiques modernes offrent une grande quantité de mémoire dédiée, elles permettent de créer des bureaux virtuels de grande taille. Notez que vous ne pourrez peut-être plus utiliser de fonctionnalités 3D si vous remplissez pratiquement toute la mémoire graphique avec le bureau virtuel. Si la carte dispose par exemple de 16 Mo de RAM vidéo, l'écran virtuel peut atteindre une taille de 4096x4096 pixels avec une profondeur de couleur de 8 bits. Il est cependant vivement recommandé, spécialement pour les cartes accélérées, de ne pas utiliser l'intégralité de la mémoire de la carte vidéo pour l'écran virtuel, puisque l'espace–mémoire non utilisé sur la carte vidéo est utilisé pour différents jeux de caractères graphiques.

11.2.2 Section Device

Une section Device décrit une carte graphique précise. Il peut y avoir un nombre quelconque de sections Device dans `xorg.conf`, tant que leurs noms, indiqués par le mot-clé `Identifier` se différencient. En règle générale—si vous avez installé plusieurs cartes graphiques—les sections sont simplement numérotées. La première est désignée par `Device[0]`, la seconde par `Device[1]`, etc. Vous voyez dans le fichier suivant l'extrait d'une section `Device` pour un ordinateur dans lequel est installée une carte graphique Matrox Millennium PCI :

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"
  Driver        "mga"
  Identifier    "Device[0]"
  VendorName    "Matrox"
  Option        "sw_cursor"
EndSection
```

Si vous utilisez SaX2 pour la configuration, la section Device devrait ressembler, à peu de choses près, à ce qui est décrit ci-dessus. En particulier,`Driver` et `BusID` dépendent bien sûr du matériel installé sur votre ordinateur et sont définis automatiquement par SaX2. Le `BusID` détermine l'emplacement PCI ou AGP dans lequel la carte graphique est enfichée. Celui-ci correspond à l'identificateur (ID) fourni par la commande lspci. Notez que le serveur X affiche les données en notation décimale, alors que le programme lspci les affiche en notation hexadécimale.

Avec le paramètre `Driver`, vous définissez le pilote à utiliser pour la carte graphique. Dans le cas de la carte Matrox Millennium, le module pilote s'appelle `mga`. Le serveur X recherche ce module dans le sous-répertoire `Drivers` via le `ModulePath`défini dans la section `Files`. Dans une installation par défaut, c'est le répertoire `/usr/X11R6/lib/modules/drivers`. Le nom est simplement suivi de `_drv.o` ; ainsi, dans le cas du pilote `mga`, le fichier pilote `mga_drv.o` est chargé.

Le comportement respectif du serveur X ou du pilote peut être influencé par des options supplémentaires. Dans la section Device, l'option `sw_cursor` est proposée à titre d'exemple. Cette option désactive le curseur matériel de la souris et représente le pointeur au niveau logiciel. Suivant le module pilote, vous disposez de différentes options que vous trouverez dans les fichiers de description des modules pilote dans le répertoire `/usr/X11R6/lib/X11/doc`. Vous trouverez également les options valables en général dans les pages de manuel (`man xorg.conf` et `man X.Org`).

11.2.3 Section Monitor et Modes

Les sections `Monitor` et `Modes` décrivent, comme les sections `Device`, chacune un écran. Le fichier de configuration `/etc/X11/xorg.conf` peut comporter autant de sections `Monitor` que nécessaires. Il est ensuite établi dans la section ServerLayout quelle section `Monitor` est concernée.

Les définitions d'écran ne doivent être définies que par des utilisateurs expérimentés. Les Modelines constituent une partie importante de la section `Monitor`. Les fréquences de synchronisation horizontales et verticales pour chaque résolution y sont définies. Les propriétés de l'écran, en particulier les fréquences de balayage autorisées sont renseignées dans la section `Monitor`.

Avertissement

Il est préférable de ne rien changer aux modelines si on ne dispose pas d'une connaissance fondamentale du fonctionnement de l'écran et de la carte graphique, car cela pourrait, dans certains cas, infliger de sérieux dommages à votre écran.

Avertissement

Ceux qui se font suffisamment confiance pour développer leurs propres configurations d'écran doivent se familiariser avec la documentation du répertoire `/usr/X11/lib/X11/doc`. La section qui traite des modes vidéo est particulièrement intéressante. Elle décrit en détail le fonctionnement du matériel et la création de modelines.

Heureusement, il n'est aujourd'hui quasiment jamais nécessaire d'établir manuellement des modelines. Si vous utilisez un écran multisync moderne, les domaines de fréquences et les résolutions optimales peuvent, en règle générale, être directement lus depuis l'écran via le DDC du serveur X, comme cela est mentionné dans la section de configuration SaX2. Si cela n'est pas possible, vous pouvez aussi utiliser un des modes VESA pré-configurés du serveur X. Cela devrait fonctionner sans problèmes sur presque toutes les combinaisons carte graphique/écran.

11.3 Installation et configuration de polices de caractères

L'installation de polices supplémentaires sous SUSE LINUX est très simple. Il suffit de copier les polices dans un répertoire qui se trouve dans le chemin désignant les polices pour X11 (voir la section 11.3.2 page 254) et qui doit être un sous-répertoire des répertoires configurés dans le fichier `/etc/fonts/fonts.conf` (voir la section 11.3.1 page ci-contre).

Vous pouvez copier manuellement (en tant que `root`) les fichiers de police dans un répertoire répondant à ces critères, par exemple `/usr/X11R6/lib/X11/fonts/truetype`. Vous pouvez aussi utiliser le programme d'installation de police de KDE du centre de contrôle KDE. Le résultat est identique.

Naturellement, vous pouvez tout aussi bien créer des liens symboliques plutôt que de copier effectivement les polices. Par exemple, lorsque vous disposez, sur une partition Windows, de polices sous licence que vous souhaitez utiliser. Appelez ensuite la commande `SuSEconfig --module fonts`.

`SuSEconfig --module fonts` appelle le script `/usr/sbin/fonts-config` qui prend en charge la configuration des polices. Pour plus de détails sur ce script et ses effets, vous pouvez lire la page de manuel correspondante (`man fonts-config`).

Le type de police à installer n'a ici aucune importance, la procédure d'installation reste identique pour les polices Bitmap, les polices TrueType et OpenType et les polices (PostScript) Type 1. Tous ces types de police peuvent être installés dans un répertoire quelconque. Les polices codées en CID représentent la seule exception. Pour ce cas, reportez-vous à la section 11.3.3 page 256.

X.Org contient deux systèmes de police totalement différents, d'une part le déjà ancien *Système de polices X11 de base*, d'autre part le tout nouveau système *Xft et fontconfig*. Dans ce qui suit, vous trouverez une courte présentation des deux systèmes.

11.3.1 Xft

Dès le début de la conception de Xft, il a été apporté le plus grand soin à la prise en charge des polices vectorielles, en particulier le lissage. Contrairement à la gestion effectuée par le système de polices X11 de base, lorsque l'on utilise Xft, c'est le programme utilisant les polices qui effectue lui-même le rendu, et non le serveur X. Ainsi, le programme en question accède aux fichiers de polices lui-même, et contrôle les moindres détails de rendu des caractères. D'une part, cela permet une représentation correcte de caractères dans de nombreuses langues, d'autre part, l'accès direct aux fichiers de polices est particulièrement intéressant pour inclure (en anglais to embed) les polices à l'impression et ainsi obtenir un résultat sur papier équivalent à ce qu'on observe sur l'écran.

Par défaut, sous SUSE LINUX, les deux environnements de bureau KDE et GNOME, Mozilla et de nombreuses autres applications utilisent déjà Xft. Xft est ainsi d'ores et déjà utilisé par un nombre d'applications bien plus important que l'ancien système de polices X11 de base.

Xft utilise la bibliothèque fontconfig pour trouver les polices ainsi que pour influer sur l'art et la manière dont elles sont rendues. Le comportement de fontconfig est dirigé par le fichier de configuration `/etc/fonts/fonts.conf`, qui s'étend à l'ensemble du système, et par le fichier de configuration `~/.fonts.conf` qui est spécifique à l'utilisateur. Chacun de ces fichiers de configuration fontconfig doit commencer par

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

et finir par

```
</fontconfig>
```

Pour indiquer les répertoires dans lesquels aller chercher les polices, vous pouvez saisir des lignes telles que :

```
<dir>/usr/local/share/fonts/</dir>
```

Ceci est toutefois rarement nécessaire. Le répertoire `~/.fonts`, propre à l'utilisateur, est déjà renseigné par défaut dans `/etc/fonts/fonts.conf`. Lorsqu'un utilisateur souhaite installer des polices pour son usage personnel, il lui suffit donc de les copier dans le répertoire `~/.fonts`.

Vous pouvez également introduire des règles pour modifier l'apparence des polices, par exemple

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

pour désactiver le lissage pour l'ensemble des polices, ou bien

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

lorsque vous ne souhaitez le désactiver que pour des polices bien définies.

La plupart des applications utilisent par défaut les noms de police `sans-serif` (ou son équivalent `monospace`), `serif` ou `monospace`. Ce ne sont pas des polices réelles mais simplement des redirections qui pointent vers les polices appropriées en fonction de la langue configurée.

Chaque utilisateur peut ainsi intégrer à son fichier `~/.fonts.conf` des règles simples pour faire pointer ces redirections vers ses polices favorites :

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Comme la plupart des applications utilisent par défaut ce système de redirection, ces règles peuvent s'appliquer à la quasi-totalité du système. Ainsi, vous pouvez utiliser presque partout vos polices préférées sans avoir à modifier individuellement la configuration de chaque programme.

Pour obtenir une liste des polices installées et disponibles, vous pouvez utiliser la commande `fc-list`. `fc-list ""` renvoie par exemple la liste de toutes les polices. Si vous souhaitez connaître les polices vectorielles (`:outline=true`) disposant de tous les caractères hébraïques (`:lang=he`) disponibles dans le système, et que vous voulez obtenir, pour chacune de ces polices, le nom (`family`), le style (`style`), la graisse (`weight`) et le nom du fichier contenant cette police, vous pouvez utiliser par exemple la commande suivante :

```
fc-list ":lang=he:outline=true" family style weight file
```

Le résultat d'une telle commande pourrait avoir l'allure suivante :

```
/usr/X11R6/lib/X11/fonts/truetype/FreeSansBold.ttf: FreeSans:style=Bold:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSerif.ttf: FreeSerif:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeMono.ttf: FreeMono:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSans.ttf: FreeSans:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

Les paramètres essentiels pouvant être utilisés avec `fc-list` sont :

TAB. 11.3: *Paramètres possibles pour fc-list*

Paramètre	Signification et valeurs possibles
family	Nom de la famille de police, par exemple `FreeSans`
foundry	Société ayant produit la police, par exemple `urw`
style	Style de la police, par exemple `Medium`, `Regular`, `Bold`, `Italic`, `Heavy`.
lang	Langues prises en charge par la police ; par exemple `fr` pour le français, `ja` pour le japonais, `zh-TW` pour le chinois traditionnel ou `zh-CN` pour le chinois simplifié.
weight	*Graisse* de la police, par exemple `80` pour une police maigre, `200` pour une police grasse.
slant	*Degré de cursivité*, principalement `0` pour une fonte non cursive, `100` pour une fonte italique.
file	Nom du fichier contenant la police
outline	`true` s'il s'agit d'une police "outline", `false` sinon.
scalable	`true` s'il s'agit d'une police vectorielle, `false` sinon.
bitmap	`true` s'il s'agit d'une police bitmap, `false` sinon.
pixelsize	Taille de la police en pixels. Cette option utilisée avec fc-list n'a de sens que pour les polices bitmap.

11.3.2 Polices X11 de base

Actuellement, le système de polices X11 de base prend en charge non seulement les polices bitmap, mais aussi les polices vectorielles telles que les polices Type1, les polices TrueType et OpenType ou encore les polices codées en CID. Les polices unicode sont également déjà prises en charge depuis longtemps. À l'origine, le système de polices X11 de base a été développé en 1987 pour X11R1 afin de gérer les polices bitmap monochromes. On constate que, jusqu'à aujourd'hui, toutes les extensions mentionnées ci-dessus ont été introduites ultérieurement dans le système.

Ainsi, par exemple, les polices vectorielles ne sont prises en charge que sans lissage et sans rendu à précision subpixel et le chargement de polices vectorielles de

grande taille, gérant les caractères pour plusieurs langues, peut être particulièrement long. L'utilisation de polices Unicode peut aussi s'avérer lent et utiliser plus de mémoire.

Le système de polices X11 de base possède quelques faiblesses de fond. On peut raisonnablement dire qu'il a vieilli et qu'il n'est plus sensé de chercher à développer des extensions. Pour des raisons de compatibilité ascendante, il reste disponible, mais il est conseillé d'utiliser, dès que possible, le système Xft et fontconfig, bien plus moderne.

Pour son fonctionnement, le serveur X doit savoir quelles polices sont disponibles et où elles se trouvent dans le système. Ceci est géré par la variable FontPath qui contient le chemin d'accès de tous les répertoires de fontes du système valides. Dans chacun de ces répertoires, un fichier nommé `fonts.dir` répertorie les fontes disponibles dans ce répertoire. FontPath est générée par le serveur X au démarrage et recherche un fichier `fonts.dir` valide dans chacune des entrées `FontPath` dans le fichier de configuration `/etc/X11/xorg.conf`. Ces entrées se trouvent dans la section `Files`. Affichez FontPath avec `xset q`. Ce chemin peut également être changé pendant le fonctionnement à l'aide de xset. Pour ajouter un chemin supplémentaire, utilisez `xset +fp <path>`. Pour supprimer un chemin non souhaité, utilisez `xset -fp <path>`.

Lorsque le serveur X est déjà lancé, des polices qui viennent d'être installées dans des répertoires déjà montés peuvent être mises à disposition à l'aide de la commande `xset fp rehash`. Cette commande est également exécutée par `SuSEconfig --module fonts`.

Comme la commande `xset` nécessite un accès au serveur X en cours d'exécution, ceci ne peut fonctionner que si `SuSEconfig --module fonts` est lancée à partir d'un interpréteur de commandes ayant un accès au serveur X qui s'exécute. Le plus simple pour parvenir à ce résultat est d'utiliser la commande `sux` et de saisir le mot de passe de root dans un terminal pour prendre la main en tant qu'utilisateur `root` : `sux` transmet à l'interpréteur root les droits de l'utilisateur ayant lancé le serveur X. Pour tester si les polices ont été installées correctement et sont disponibles dans le système de polices X11 de base, vous pouvez utiliser la commande `xlsfonts` qui dresse la liste de toutes les polices disponibles.

SUSE LINUX utilise par défaut l'encodage UTF-8 local, en conséquence, il vous est conseillé d'utiliser en règle générale les polices Unicode (noms de police reconnaissables à leur terminaison en `iso10646-1` dans la liste affichée par `xlsfonts`). Vous pouvez ainsi obtenir la liste de toutes les polices Unicode disponibles à l'aide de la commande `xlsfonts | grep iso10646-1`. La quasi-totalité des polices Unicode disponibles sous SUSE LINUX contiennent, au

moins, tous les caractères nécessaires pour les langues européennes (précédents encodages : `iso-8859-*`).

11.3.3 Polices codées en CID

Contrairement aux autres types de polices, les polices codées en CID ne peuvent pas être installées dans un répertoire quelconque. Elles doivent toujours être installées dans le répertoire `/usr/share/ghostscript/Resource/CIDFont`. Cela n'a pas d'importance pour Xft et fontconfig, en revanche Ghostscript et le système de polices X11 de base l'exigent.

Astuce

Des informations complémentaires concernant les polices sous X11 sont disponibles à l'adresse `http://www.xfree86.org/current/fonts.html`.

Astuce

11.4 Configuration de OpenGL—3D

11.4.1 Prise en charge du matériel

SUSE LINUX comprend divers pilotes OpenGL pour la prise en charge du matériel 3D. Vous trouverez un aperçu dans le tableau 11.4 de la présente page.

TAB. *11.4:* *Matériel 3D pris en charge*

Pilote OpenGL	Matériel pris en charge
nVidia	Chipset nVidia : tous sauf Riva 128(ZX)
DRI	3Dfx Voodoo Banshee, 3Dfx Voodoo-3/4/5, Intel i810/i815/i830M, Intel 845G/852GM/855GM/865G,915, Matrox G200/G400/G450/G550, ATI Rage 128(Pro)/Radeon (jusqu'à 9250)

Lors d'une première installation avec YaST, l'accélération 3D peut être activée dès l'installation, si YaST offre la prise en charge correspondante. En présence de composants graphiques nVidia, il faut d'abord installer le pilote nVidia. Pour cela, choisissez pendant l'installation le correctif du pilote nVidia dans YOU (YaST Online Update). Nous ne pouvons malheureusement pas vous fournir le pilote nVidia pour des questions de licence.

Si une mise à jour a été installée, la prise en charge du matériel 3D doit être configurée de manière différente. La procédure dépend là du pilote OpenGL à utiliser et est expliquée plus précisément dans la section suivante.

11.4.2 Pilote OpenGL

Ces pilotes OpenGL peuvent être aisément configurés avec SaX2. Notez que pour des cartes nVidia, le pilote nVidia doit être installé au préalable (voir plus haut). Utilisez la commande `3Ddiag` pour vérifier si la configuration de nVidia ou DRI est correcte.

Pour des raisons de sécurité, seuls les utilisateurs du groupe `video` ont accès au matériel 3D. Assurez-vous par conséquent que tous les utilisateurs travaillant localement sur l'ordinateur sont enregistrés dans ce groupe. Sinon, on utilise, pour les programmes OpenGL, le plus lent *Software Rendering Fallback* du pilote OpenGL. Utilisez la commande `id` pour vérifier si l'utilisateur actuel appartient au groupe `video`. Si ce n'est pas le cas, vous pouvez l'ajouter à ce groupe avec YaST.

11.4.3 Outil de diagnostic 3Ddiag

Pour pouvoir vérifier la configuration 3D sous SUSE LINUX, vous disposez de l'outil de diagnostic 3Ddiag. Veuillez noter qu'il s'agit d'un outil en ligne de commande que vous devez utiliser dans un terminal. Saisissez `3Ddiag -h` pour afficher les possibles options de 3Ddiag.

Pour vérifier la configuration de X.Org, le programme s'assure que les paquetages nécessaires à la prise en charge 3D sont installés et si la bibliothèque OpenGL ainsi que l'extension GLX correctes sont utilisées. Veuillez suivre les instructions de 3Ddiag quand apparaissent des messages "failed". En cas de succès, seuls des messages "done" sont affichés à l'écran.

11.4.4 Programmes test pour OpenGL

Outre `glxgears`, des jeux comme `tuxracer` et `armagetron` (paquetage du même nom) conviennent bien comme programmes de test pour OpenGL. Si la prise en charge de la 3D est activée, ils s'affichent de manière fluide sur l'écran d'un ordinateur à peu près actuel. Sans prise en charge de la 3D, ceci est insensé (effet diapositives). L'affichage de `glxinfo` informe précisément de l'état d'activation de la prise en charge de la 3D. Si elle est bien activée, le résultat contiendra la ligne `direct rendering: Yes`.

11.4.5 Dépannage

Si le résultat du test 3D OpenGL s'avère être négatif, (pas de jeu fluide possible), vérifiez d'abord avec 3Ddiag s'il n'existe pas d'erreur de configuration (messages "failed"). Si leur correction ne résout pas le problème, cela ne change rien ou s'il n'y avait aucun message "failed", il suffit souvent de consulter les fichiers Log de X.Org. Ici, on trouve souvent dans `/var/log/Xorg.0.log` de X.Org la ligne `DRI is disabled`. Il peut y avoir plusieurs causes que l'on ne peut cependant trouver qu'en effectuant un examen précis du fichier journal, ce qui souvent dépasse le débutant.

Dans ces cas, il ne s'agit pas en règle générale d'une erreur de configuration puisque celle-ci aurait déjà été détectée par 3Ddiag. Donc, la seule solution encore possible est d'utiliser le Software Rendering Fallback du pilote DRI, qui n'offre cependant aucune prise en charge de la 3D. De même, il vaut mieux renoncer à l'utilisation de la prise en charge de la 3D quand surviennent des erreurs de représentation OpenGL ou même des problèmes de stabilité. Utilisez SaX2 pour désactiver la prise en charge de la 3D.

11.4.6 Assistance à l'installation

Outre le `Software Rendering Fallback` du pilote DRI, tous les pilotes OpenGL sous Linux sont encore en développement et doivent donc être considérés comme des pilotes expérimentaux. Nous avons cependant pris la décision de fournir les pilotes dans cette distribution, car il y a une grosse demande d'accélération matérielle 3D sous Linux. En raison du stade actuel expérimental des pilotes OpenGL, nous ne pouvons cependant pas étendre le cadre de l'assistance à l'installation à la configuration de l'accélération matérielle 3D et ne pouvons pas vous venir en aide en cas de problèmes s'y rapportant. L'installation de base

de l'interface utilisateur graphique X11 ne comprend donc en aucun cas aussi l'installation de l'accélération matérielle 3D. Cependant nous espérons que ce chapitre a déjà répondu à beaucoup de vos questions à ce sujet. Si vous rencontrez des problèmes avec la prise en charge du matériel 3D, nous vous conseillons, en cas de doute, de vous passer de cette prise en charge.

11.4.7 Documentation en ligne additionnelle

Des informations sur DRI sont disponibles dans `/usr/X11R6/lib/X11/doc/README.DRI` (`xorg-x11-doc`). Vous trouverez des informations sur l'installation du pilote nvidia sous `http://ftp.suse.com/pub/suse/i386/supplementary/X/nvidia-installer-HOWTO.html`.

Utilisation de l'imprimante

Dans ce chapitre nous abordons des connaissances de base sur le fonctionnement de l'imprimante. Ce chapitre sert aussi en particulier à apporter des solutions appropriées aux problèmes de fonctionnement des imprimantes en réseau.

12.1 Préparatifs et autres considérations

CUPS est le système d'impression par défaut sous SUSE LINUX. CUPS est très "orienté utilisateur". Dans de nombreux cas, il est compatible avec LPRng ou peut le devenir de façon relativement aisée. Ce n'est que pour des raisons de compatibilité que LPRng est compris dans SUSE LINUXSUSE LINUX Enterprise ServerNovell Linux Desktop

Les imprimantes se distinguent par leur interface, USB ou réseau, ainsi que par leur langage d'impression. Lors de l'achat d'une imprimante, il convient d'accorder de l'importance tant à une interface appropriée prise en charge par le matériel, qu'au langage d'impression. On peut, pour simplifier, répartir les imprimantes dans les trois catégories suivantes de langages d'impression :

Imprimantes PostScript PostScript est le langage d'impression dans lequel la plupart des travaux d'impression sous Linux/Unix sont générées et traités en interne par le système d'impression. Ce langage, très puissant, est déjà ancien. Lorsque les documents PostScript peuvent être traités directement par l'imprimante et ne nécessitent pas d'étapes de transformation supplémentaires au sein du système d'impression, le nombre de sources d'erreur potentielles s'en trouve réduit. Comme les imprimantes PostScript sont soumises à une licence et que les coûts qui en découlent ne sont pas négligeables, ces imprimantes sont généralement plus onéreuses que les imprimantes non dotées d'un interpréteur PostScript.

Imprimantes usuelles (langages comme PCL et ESC/P)
Ces langages d'impression existent depuis longtemps, mais sont encore aujourd'hui étendus pour pouvoir s'adapter aux dernières évolutions des imprimantes. Lorsqu'il s'agit de langages d'impression usuels, les travaux du système d'impression PostScript peuvent être transformés à l'aide de Ghostscript dans le langage d'impression (on dit "interprétés"). Les langages les plus connus sont PCL, que l'on trouve essentiellement dans les imprimantes HP et leurs "clones" ainsi que ESC/P, répandu dans les imprimantes Epson. On peut partir du principe que ce type de langages d'impression donnera aussi de bons résultats d'impression sous Linux. À part les pilotes `hpijs` développés par la société HP elle-même, il n'existe actuellement aucun fabricant d'imprimantes qui développe des pilotes pour Linux et les met à la disposition des distributeurs Linux sous une licence OpenSource. Les imprimantes de cette catégorie se situent le plus souvent dans une fourchette de prix moyenne.

Imprimantes propriétaires (imprimantes GDI, le plus souvent)
Dans la catégorie des imprimantes propriétaires, il existe normalement un ou plusieurs pilotes Windows. Avec ces imprimantes, aucun langage d'impression usuel n'est pris en charge et le langage d'impression qu'elles utilisent peut varier d'une version du modèle d'imprimante à une autre. Pour plus d'informations sur cette problématique, reportez-vous à la section 12.8.1 page 279.

Avant d'acheter une nouvelle imprimante, consultez les sources d'information suivantes afin de vérifier le degré de prise en charge de l'imprimante choisie :

- `http://cdb.suse.de/`—la base de données d'imprimantes de SUSE LINUX
- `http://www.linuxprinting.org/`—la base de données d'imprimantes sur Linuxprinting.org
- `http://www.cs.wisc.edu/~ghost/`—la page d'accueil de Ghostscript
- `/usr/share/doc/packages/ghostscript/catalog.devices`—les pilotes intégrés

Il va de soi que les bases de données en ligne indiquent toujours l'état actuel de la prise en charge sous Linux. Cependant, une distribution Linux ne peut pas offrir un pilote publié après sa date de fabrication ; il est donc possible qu'une imprimante actuellement classée comme "parfaitement prise en charge" ne l'ait en fait pas encore été au moment de la production de SUSE LINUX. Les bases de données n'indiquent donc pas nécessairement l'état correct, mais plutôt une bonne approximation.

12.2 Déroulement du travail d'impression sous Linux

L'utilisateur génère un nouveau travail d'impression. Le travail d'impression se compose des données à imprimer plus des informations pour le spouleur, telles que le nom de l'imprimante ou le nom de la file d'attente et, optionnellement, les informations pour le filtre d'impression telles que les options spécifiques à l'imprimante.

Pour chaque imprimante, il existe une file d'attente qui lui est propre. Le spouleur d'impression conserve le travail d'impression jusqu'à ce que l'imprimante concernée soit prête à recevoir des données. Lorsque l'imprimante est prête, le spouleur lui envoie les données à traver le filtre et le backend.

Le filtre convertit les données que l'utilisateur souhaite imprimer (ASCII, PostScript, PDF, JPEG, etc.) en données spécifiques à l'imprimante (PostScript, PCL, ESC/P, etc.). Les caractéristiques de l'imprimante sont décrites dans les fichiers PPD. Un fichier PPD contient des options spécifiques à l'imprimante avec les paramètres nécessaires afin de les activer pour l'imprimante. Les système de filtre vous assure que les options que vous avez sélectionnées sont activées.

Si vous utilisez une imprimante PostScript, le système filtre convertit les données en données PostScript adaptées à l'imprimante. Ceci ne nécessite pas un pilote d'imprimante. Si ce n'est pas une imprimante PostScript qui est connectée, le système filtre utilise le programme Ghostscript pour convertit les données en données adaptées à l'imprimante. Ceci nécessite un pilote Ghostscript adapté au modèle d'imprimante utilisé. Le backend reçoit du filtre les données adaptées à l'imprimante, lesquelles sont ensuite envoyées à l'imprimante.

12.3 Méthodes et protocoles pour le raccordement des imprimantes

On peut raccorder une imprimante au système de plusieurs façons. Avec le système d'impression CUPS, le fait qu'une imprimante soit reliée au système en local ou en réseau n'a pas d'influence sur la configuration. Sous Linux, les imprimantes locales sont connectées exactement comme le décrit le manuel fourni par le fabricant de l'imprimante. CUPS prend en charge les connexions série, USB, parallèle et SCSI. Pour plus d'informations en ce qui concerne le raccordement des imprimantes, lisez également l'article présentant des notions de base *CUPS in a Nutshell* (en anglais) dans la base de données support à l'adresse `http://portal.suse.com`. Indiquez *cups* dans le formulaire de recherche.

Avertissement

Raccordement par câble à l'ordinateur

Lors du câblage de l'imprimante à l'ordinateur, il faut savoir que seules les périphériques USB sont prévus pour être connectés ou déconnectés en cours de fonctionnement. On ne devrait modifier les autres branchements que lorsque l'ordinateur est éteint.

Avertissement

12.4 Installation du logiciel

"PostScript Printer Description" (PPD) est le langage informatique qui décrit les propriétés, telles que la résolution, et les options, telles que le mode duplex, des imprimantes. Ces decriptions sont nécessaires pour pouvoir utiliser les différentes options de l'imprimante sous CUPS. Sans fichier PPD, les données d'impression sont transmises à l'imprimante à l'état "brut", ce qui n'est en général pas souhaitable. Avec SUSE LINUX, beaucoup de fichiers PPD sont pré-installés afin de pouvoir utiliser même des imprimantes qui ne prennent pas en charge PostScript.

Avec une imprimante PostScript, il est recommandé de se procurer le fichier PPD approprié ; le paquetage `manufacturer-PPDs` en contient une multitude qui sont installés automatiquement lors d'une installation standard. Voir la section 12.7.4 page 276 et la section 12.8.2 page 279.

On peut placer les nouveaux fichiers PPD dans le répertoire `/usr/share/cups/model/` ou les ajouter avec YaST (voir la section Configuration manuelle page suivante). Un tel fichier PPD peut alors être sélectionné lors de l'installation.

La prudence est cependant de mise si un fabricant d'imprimantes demande non seulement de modifier les fichiers de configuration mais également d'installer des paquetages logiciels complets. D'une part, une telle installation vous fait perdre l'assistance technique que vous offre SUSE LINUX et d'autre part, il se peut que les commandes d'impression ne fonctionnent plus comme auparavant et qu'il ne soit plus possible de piloter des périphériques provenant d'autres fabricants. C'est pourquoi il est en général déconseillé d'installer les logiciels fournis par les fabricants.

12.5 Configuration de l'imprimante

Après avoir connecté l'imprimante à l'ordinateur et installé le logiciel, il faut configurer l'imprimante au niveau du système. Si possible, n'utilisez pour cela que les outils fournis avec SUSE LINUX. Comme la sécurité est très importante pour SUSE LINUX, les outils provenant de tiers ne sont pas toujours adaptés aux restrictions imposées par la sécurité et s'avérent ainsi souvent plus problématiques qu'utiles.

12.5.1 Imprimantes locales

Si, lorsque vous vous connectez, une imprimante locale qui n'a pas encore été configurée est détectée, YaST est lancé afin de pouvoir procéder à la configuration. Cela passe par les mêmes dialogues que dans le cas de la configuration décrite ci-après.

Pour configurer l'imprimante, sélectionnez 'Matériel' → 'Imprimante' dans le Centre de Contrôle YaST. La fenêtre principale de configuration des imprimantes s'ouvre. La liste des imprimantes reconnues est affichée dans la partie supérieure tandis que les files d'attente déjà configurées s'affichent dans la partie inférieure. Si votre imprimante n'a pas été reconnue automatiquement, configurez-la manuellement.

Important

Si l'entrée 'Imprimante' n'est pas disponible dans le centre de contrôle de YaST, c'est très probablement que le paquetage `yast2-printer` n'est pas installé. Pour résoudre ce problème, installez-le et redémarrez YaST.

Important

Configuration automatique

YaST permet de configurer automatiquement l'imprimante lorsque le port parallèle ou USB peut être configuré automatiquement de façon correcte et que l'imprimante qui y est connectée a été reconnue automatiquement. La base de données des imprimantes contient l'identification du modèle d'imprimante que YaST a obtenu lors de la reconnaissance automatique du matériel. Pour certaines imprimantes, ce matériel identifié peut différer du nom du modèle. Dans ce cas, sélectionnez le modèle manuellement.

Chaque configuration devrait faire l'objet d'une vérification à l'aide du test d'impression de YaST pour s'assurer qu'elle fonctionne réellement. De plus, la page de test de YaST vous fournit également des informations importantes sur la configuration en question.

Configuration manuelle

Lorsqu'une des conditions requises pour la configuration automatique n'est pas remplie ou que l'on souhaite une configuration particulière donnée, celle-ci doit se faire manuellement. Selon la réussite de la reconnaissance automatique et la

quantité d'informations contenues dans la base de données des imprimantes sur le modèle d'imprimante choisi, YaST peut être capable de déterminer automatiquement les paramètres corrects ou, pour le moins, de proposer une présélection rationnelle.

Les paramètres suivants doivent être configurés :

Connexion matérielle (interface) La configuration de la connexion matérielle dépend de si YaST a pu détecter l'imprimante lors de la reconnaissance automatique du matériel. Si YaST peut reconnaître automatiquement le modèle de l'imprimante, on peut partir du principe que la connexion matérielle avec l'imprimante fonctionne et qu'il n'y a donc rien à régler de ce point de vue. Si YaST n'est pas en mesure de reconnaître automatiquement le modèle de l'imprimante, il est possible que la connexion de l'imprimante au niveau matériel ne fonctionne pas et qu'une intervention manuelle soit nécessaire pour configurer la connexion.

Nom de la file d'attente Le nom de la file d'attente est utilisé dans les commandes d'impression. Le nom doit donc être relativement court et ne contenir que des lettres minuscules et des chiffres.

Modèle d'imprimante et fichier PPD Les paramètres propres à l'imprimante, tels que le pilote Ghostscript à utiliser et les paramètres du filtre d'impression pour le pilote, sont enregistrés dans un fichier PPD (en anglais, PostScript Printer Description "description d'imprimante PostScript"). Pour plus d'informations sur les fichiers PPD, reportez-vous à la section 12.4 page 265.

Pour de nombreux modèles d'imprimantes, on dispose de plusieurs fichiers PPD, par exemple lorsque plusieurs pilotes Ghostscript fonctionnent avec le modèle en question. Si vous sélectionnez le fabricant et le modèle, YaST choisit ensuite le fichier PPD approprié. Si l'on dispose de plusieurs fichiers PPD, YaST en choisit un par défaut (normalement celui qui est mis en évidence par la mention `recommended`). On changer le fichier PPD par défaut au moyen de 'Modifier'.

Pour les imprimantes non PostScript, les données adaptées à l'imprimante sont générées par l'intermédiaire d'un pilote Ghostscript. Ainsi, la configuration du pilote Ghostscript est le facteur décisif pour déterminer la qualité de l'impression. C'est le pilote Ghostscript sélectionné (via fichier PPD) et les options qui lui sont propres qui déterminent les caractéristiques de l'impression. Si nécessaire, vous pouvez changer d'autres options (disponibles dans le fichier PPD) en sélectionnant 'modifier'.

L'impression de la page de test est indispensable afin de vous assurer que vos réglages fonctionnent correctement. Si, lors de cette opération, la page

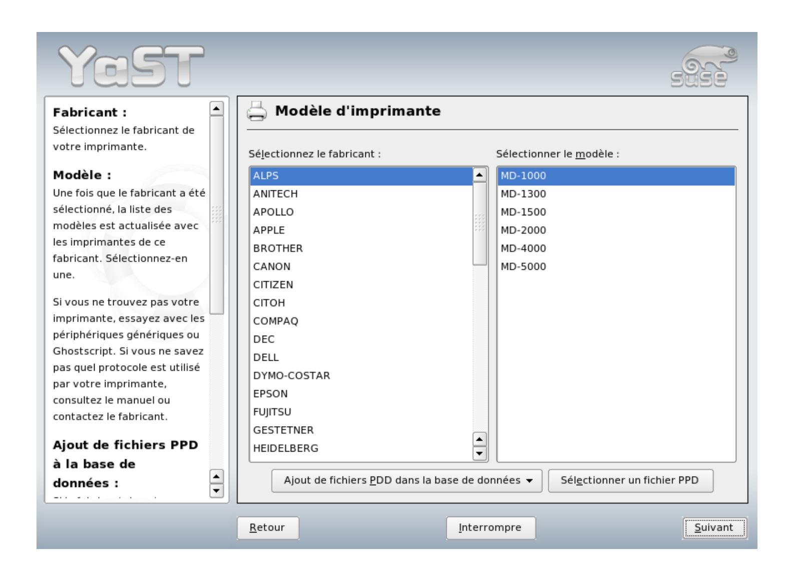


FIG. *12.1: Sélection du modèle d'imprimante*

de test ne contient que des caractères incompréhensibles ou, par exemple, beaucoup de pages vides, vous pouvez arrêter immédiatement l'impression au niveau de l'imprimante, en retirant tout le papier puis en interrompant le test d'impression dans YaST.

Si le modèle de l'imprimante ne figure pas dans la base de données des imprimantes, vous pouvez ajouter un nouveau fichier PPD en sélectionnant 'Ajouter fichier PPD à la base de données'ou utiliser une collection de fichiers PPD génériques pour les langages d'impression usuels. Prenez alors comme "fabricant" 'UNKNOWN MANUFACTURER'.

Paramètres avancés Vous n'avez normalement aucun changement à faire.

Configuration avec les outils en mode ligne de commande

Pour configurer l'imprimante par l'intermédiaire des outils en ligne de commande décrits dans la section Configuration avec les outils en mode ligne de commande page 270, il vous faut un URI (uniform resource identifier) de périphérique qui consiste en un backend tel que usb et des paramètres tels que /dev/usb/lp1. L'URI complet peut, par exemple, avoir la forme `parallel:/dev/lp0` (imprimante connectée au premier port parallèle) ou `usb:/dev/usb/lp0` (première imprimante connectée au port USB).

12.5.2 Imprimantes réseau

Une imprimante réseau est capable de prendre en charge plusieurs protocoles, certains même simultanément. La plupart des protocoles reconnus sont standardisés, il n'est pourtant pas exclu que le standard soit étendu (modifié) par les fabricants, soit parce qu'ils testent sur des systèmes sous lesquels le standard n'est pas correctement implémenté, soit parce qu'ils souhaitent certaines fonctions qui n'existent pas dans le standard. Les fabricants n'offrent de tels pilotes que pour certains systèmes d'exploitation, dont Linux fait malheureusement rarement partie. Pour le moment, on ne peut pas considérer que tous les protocoles fonctionnent sous Linux sans poser de problèmes, et il convient d'expérimenter différentes possibilités afin d'obtenir une configuration qui fonctionne.

Sous CUPS, les protocoles `socket`, `LPD`, `IPP` et `smb` sont pris en charge. Vous trouverez ci-après quelques informations détaillées concernant ces protocoles :

socket On désigne sous le nom de *socket* une liaison dans laquelle les données sont envoyées sur un socket internet sans prise de contact (handshake) préalable. Les numéros de port socket typiquement utilisés sont `9100` ou `35`. Un exemple d'URI de périphérique est `socket://host-printer:9100/`.

LPD (Line Printer Daemon) Le protocole LPD est traditionnellement éprouvé. LPD signifie "Line Printer Daemon" et est décrit dans le RFC 1179. Sous ce protocole, quelques données concernant le travail, telles que l'identificateur de la file d'attente de l'imprimante sont envoyées avant l'envoi des données d'impression proprement dites. C'est la raison pour laquelle il est nécessaire d'indiquer également une file d'attente lors de la configuration du protocole LPD pour la transmission de données. Les implémentations de divers fabricants d'imprimantes sont réalisées de façon tellement souple qu'elles acceptent n'importe quel nom de file d'attente. En cas de besoin, le nom à utiliser se trouve dans le manuel d'utilisation de l'imprimante. Très souvent, les noms sont LPT, LPT1, LP1 ou des noms du même genre. Il est bien sûr possible de configurer de la même manière une file d'attente LPD sur un autre hôte Linux ou Unix dans le système CUPS. Le numéro de port du service LPD est `515`. Voici un exemple d'URI de périphérique : `lpd://host-printer/LPT1`

IPP (Internet Printing Protocol) Le protocole d'impression Internet, IPP, est encore relativement récent (1999) et est basé sur le protocole HTTP. IPP est le protocole le plus utilisé pour envoyer les données concernant le travail. CUPS se sert de IPP pour la transmission interne des

données. C'est le protocole de choix si l'on souhaite établir une file d'attente de redirection entre deux serveurs CUPS. Ici encore, le nom de la file d'attente d'impression est nécessaire afin de pouvoir configurer correctement IPP. Le numéro de port pour IPP est `631`. Voici des exemples d'URI de périphérique : `ipp://host-printer/ps` et `ipp://host-cupsserver/printers/ps`

SMB (partage Windows) CUPS prend également en charge l'impression sur des imprimantes connectées sur des partages Windows. Le protocole correspondant est SMB qui utilise les numéro de port `137`, `138` et `139`. Voici des exemples d'URI de périphérique : `smb://user:password@workgroup/server/printer`, `smb://user:password@host/printer` et `smb://server/printer`

Avant de procéder à la configuration, il faut par conséquent déterminer le protocole reconnu par l'imprimante. S'il n'est pas indiqué par le fabricant, il est possible de le rechercher en saisissant la commande `nmap` qui accompagne le paquetage `nmap`. `nmap` examine un hôte pour trouver des ports ouverts. Par un exemple :

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

12.5.3 Opérations de configuration

Il est possible de procéder à des opérations de configuration à l'aide de YaST ou d'outils en ligne de commande.

Configuration de CUPS en réseau au moyen de YaST

Il est conseillé de procéder à la configuration des imprimantes réseau en utilisant YaST. YaST facilite la configuration et les limitations imposées par la sécurité de CUPS ne lui posent aucun problème (voir la section 12.7.2 page 274).

Pour plus d'informations relatives à l'installation de CUPS en réseau, veuillez lire l'article présentant des notions de base *CUPS in a Nutshell* (en anglais) dans la base de données support à l'adresse `http://portal.suse.com`.

Configuration avec les outils en mode ligne de commande

Une autre variante consiste à configurer CUPS par l'intermédiaire des outils de la ligne de commande tels que `lpadmin` et `lpoptions`. Si tout est déjà préparé (si vous connaissez le fichier PPD et le nom du périphérique), il suffit de procéder comme suit :

```
lpadmin -p file_d_attente -v URI_de_périphérique \
-P fichier PPD -E
```

Veillez à ce que le `-E` ne soit pas la première option car pour toutes les commandes de CUPS, `-E` en tant que premier argument signifie qu'il faut utiliser une liaison chiffrée (en anglais Encrypted) et non, comme on en a l'intention ici, activer l'imprimante (en anglais Enable). Voici un exemple concret de l'utilisation de `-E` :

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

Exemple analogue pour une imprimante réseau :

```
lpadmin -p ps -v socket://192.168.1.0:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Modifier des options

Lors de l'installation du système, certaines options sont définies par défaut. On peut modifier ces options à chaque travail d'impression (dans les limites de ce que permet l'outil d'impression utilisé). On peut aussi redéfinir ces options par défaut avec YaST. À la ligne de commande, les options par défaut sont définies comme décrit ci-après :

1. On affiche d'abord toutes les options :

   ```
   lpoptions -p file_d_attente -l
   ```

   Exemple :

   ```
   Resolution/Output Resolution: 150dpi *300dpi 600dpi
   ```

   L'option activée par défaut se reconnaît au moyen de l'astérisque qui la précède (*).
2. Modifiez ensuite l'option à l'aide de `lpadmin` :

   ```
   lpadmin -p file_d_attente -o Resolution=600dpi
   ```

3. Vérifiez les nouveaux paramètres :

   ```
   lpoptions -p file_d_attente -l
   ```

   ```
   Resolution/Output Resolution: 150dpi 300dpi *600dpi
   ```

12.6 Configuration des applications

Les applications emploient les files d'attente disponibles de la même manière que pour l'impression depuis la ligne de commande. Par conséquent, il n'est normalement pas nécessaire de reconfigurer l'imprimante pour des applications. Vous devriez pouvoir imprimer depuis des applications en utilisant les files d'attente existantes.

12.6.1 Impression depuis la ligne de commande

En mode ligne de commande, on imprime avec la commande `lp -d` ⟨*file_d_attente*⟩ ⟨*nom_du_fichier*⟩ , en remplaçant ⟨*file_d_attente*⟩ et ⟨*nom_du_fichier*⟩ comme il convient.

12.6.2 Impression en mode ligne de commande avec les applications

Certaines applications emploient la commande `lp` pour imprimer. Dans le dialogue d'impression du logiciel, saisissez la commande d'impression appropriée (sans spécifier, généralement, le ⟨*nom_du_fichier*⟩), par exemple, `lp -d` ⟨*file_d_attente*⟩ . Pour que cela fonctionne avec les programmes KDE, il activer 'Impression via un programme externe (générique)'. Sinon on ne peut pas saisir la commande d'impression.

12.6.3 Impression avec le système d'impression CUPS

Les outils tels que xpp ou le programme kprinter de KDE sont des interfaces graphiques qui permettent non seulement de choisir parmi le files d'attente, mais aussi d'ajuster les options par défaut de CUPS et les options qui sont propres à l'imprimante dans le fichier PPD. Vous pouvez utiliser kprinter comme interface d'impression standard des applications non KDE en spécifiant la commande d'impression `kprinter` ou `kprinter --stdin` dans le dialogue d'impression de ces logiciels. La commande d'impression à choisir dépend du comportement de ces logiciels. Si la configuration est correcte, l'application ouvrira le dialogue d'impression de kprinter lorsqu'un travail d'impression est donné, vous permettant ainsi de sélectionner la file d'attente ainsi que de définir d'autres options d'impression. Cependant, il faut veiller à ce que le réglage propre à l'application ne rentre pas en conflit avec celui de kprinter et que les options d'impression ne soient changées que dans kprinter une fois qu'il a été activé.

12.7 Particularités de SUSE LINUX

De nombreuses fonctionnalités CUPS ont été adaptées pour être SUSE LINUX. Quelques-unes des modifications les plus importantes sont couvertes ici.

12.7.1 Le serveur CUPS et le pare-feu

Il y a de nombreuses manières de configurer CUPS en tant que client d'un serveur réseau.

- On peut, pour chaque file d'attente sur le serveur réseau, mettre en place une file d'attente locale et transmettre par son intermédiaire tous les travaux d'impression au serveur réseau correspondant. En règle générale, cette méthode n'est pas conseillée, car si la configuration du serveur réseau est modifiée, cela nécessite de reconfigurer tous les clients.
- Il est possible de relayer des travaux d'impression directement sur un serveur réseau en particulier. Pour une telle configuration, il n'est pas nécessaire d'exécuter un démon CUPS local. La commande `lp` ou tout appel de la bibliothèque correspondante par d'autres programmes, permet d'envoyer des travaux directement au serveur réseau. Toutefois, une telle configuration ne fonctionne pas si l'on souhaite imprimer aussi sur une imprimante locale.
- Le démon CUPS peut se tenir à l'écoute de paquets de diffusion IPP envoyés par d'autres serveurs réseau qui souhaitent signaler la mise à disposition de files d'attentes. C'est la meilleure manière de régler CUPS lorsque l'on souhaite pouvoir imprimer sur des serveurs CUPS distants. Une telle configuration comporte toutefois le risque qu'un attaquant envoie au démon des diffusions IPP mentionnant des files d'attentes. Le démon local accède ensuite à ces files d'attentes contrefaites et, lorsque l'attaquant propose une file d'attente portant le même nom qu'une autre file du serveur local, et que le paquet IPP a été reçu plus tôt, alors l'utilisateur croit avoir transmis un travail au serveur local alors qu'en réalité, le travail parvient au serveur de l'attaquant. Pour utiliser cette méthode, le port UDP 631 doit être ouvert aux paquets entrants.

YaST peut trouver les serveurs CUPS en scrutant tous les hôtes réseau pour voir si elles proposent ce service ou en surveillant les diffusions IPP. Cette deuxième méthode est utilisée pendant l'installation du système pour trouver les serveurs CUPS proposés. Pour cela, le port UDP 631 doit être ouvert aux paquets entrants.

La configuration par défaut du pare-feu telle qu'elle est affichée dans le dialogue de suggestions est de rejeter les diffusions IPP sur toutes les interfaces. Cela signifie que la deuxième méthode de détection des files d'attente distantes ainsi que

la troisième méthode d'accès aux files d'attente distantes ne pourront pas fonctionner. Il est donc impératif de modifier la configuration du pare-feu en marquant l'une des interfaces comme `internal` ce qui ouvre le port par défaut ou en ouvrant de façon explicite le port d'une des interfaces ouvertes vers l'extérieur (`external`). En effet, pour des raisons de sécurité, aucun des ports n'est ouvert par défaut. Ouvrir un port afin de pouvoir configurer l'accès aux files d'attente distantes suivant la deuxième méthode peut constituer un problème de sécurité étant donné qu'un attaquant envoie des diffusions et que des utilisateurs acceptent ainsi le serveur d'un agresseur.

L'utilisateur doit modifier la configuration du pare-feu qui lui est proposée de manière à permettre à CUPS de trouver les files d'attente distantes au cours de l'installation et par la suite, en fonctionnement normal, à permettre l'accès aux différents serveurs distants depuis le système local. On peut aussi envisager que l'utilisateur détecte les serveurs CUPS en scrutant activement les ordinateurs du réseau local ou qu'il configure à la main toutes les files d'attente. Cependant, nous ne conseillons pas cette possibilitée pour les raisons évoquées auparavant.

12.7.2 Administrateur pour frontal web CUPS

Afin de pouvoir utiliser l'administration avec le frontal web (CUPS) ou avec l'outil d'administration d'imprimante (KDE), l'utilisateur `root` doit être déclaré en tant qu'administrateur CUPS avec le groupe d'administration de CUPS `sys` et un mot de passe pour CUPS. Pour cela, saisissez en tant que `root` la commande suivante :

```
lppasswd -g sys -a root
```

Si vous ne procédez pas ainsi, l'administration depuis le frontal web ou depuis l'outil d'administration ne sera pas possible car l'authentification échoue lorsqu'aucun administrateur CUPS n'a été configuré. Au lieu de `root`, on peut également définir un autre utilisateur en tant qu'administrateur CUPS (voir la section 12.7.3 page ci-contre).

12.7.3 Modifications du service d'impression CUPS (cupsd)

À l'origine, ces modifications ont été apportées pour SUSE LINUX 9.1.

cupsd fonctionne en tant qu'utilisateur lp

Au démarrage, `cupsd` passe de l'utilisateur `root` à l'utilisateur `lp`. Ceci augmente le niveau de sécurité car le service d'impression CUPS ne fonctionne pas avec des droits illimités mais uniquement avec les droits nécessaires au service d'impression.

L'inconvénient résulte cependant dans le fait que l'authentification (la vérification du mot de passe) ne peut pas s'effectuer par le biais de `/etc/shadow` étant donné que `lp` n'a pas accès à `/etc/shadow`. Ainsi, l'authentification spécifique de CUPS via `/etc/cups/passwd.md5` doit être utilisée. Pour ce faire, il faut entrer l'administrateur CUPS avec le groupe d'administration CUPS `sys` et le mot de passe CUPS dans `/etc/cups/passwd.md5`. Pour cela, saisissez en tant que `root` la commande suivante :

```
lppasswd -g sys -a <nom admin CUPS>
```

Lorsque `cupsd` fonctionne en tant que `lp`, le fichier `/etc/printcap` ne peut pas être créé, car `lp` n'est pas autorisé à créer des fichiers dans /etc/. C'est la raison pour laquelle cupsd crée `/etc/cups/printcap`. `/etc/printcap` est un lien symbolique vers `/etc/cups/printcap` afin que les programmes applicatifs qui ne peuvent lire le nom de la file d'attente que depuis `/etc/printcap` puissent continuer à fonctionner correctement.

Dès que cupsd fonctionne en tant que `lp` il est impossible d'ouvrir le port 631. C'est pourquoi cupsd ne peut plus être rechargé par le biais de `rccups reload`. Il convient dont d'utiliser `rccups restart`.

Fonctionnalité généralisée pour BrowseAllow et BrowseDeny

Les conditions d'accès configurées pour `BrowseAllow` et `BrowseDeny` se réfèrent à tous les types de paquets envoyés au démon cupsd. Les réglages par défaut dans `/etc/cups/cupsd.conf` sont :

```
BrowseAllow @LOCAL
BrowseDeny All
```

et

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

On peut ainsi accéder exactement aux ordinateurs de type `LOCAL` sur le démon cupsd à un serveur CUPS. Les ordinateurs de type `LOCAL` sont des ordinateurs dont l'adresse IP n'appartient pas à une interface point-à-point (interface dont le flag `IFF_POINTOPOINT` n'est pas à 1) et dont l'adresse IP appartient au même réseau que le serveur CUPS. Tous les autres ordinateurs rejettent immédiatement quelque paquet que ce soit.

cupsd activé par défaut

Lors d'une installation standard, `cupsd` est activé automatiquement, ce qui permet d'accéder confortablement aux files d'attente des serveurs réseau CUPS sans avoir recours à d'autres opérations manuelles. Les deux premiers points (voir la section cupsd fonctionne en tant qu'utilisateur lp page précédente et la section Fonctionnalité généralisée pour BrowseAllow et BrowseDeny page précédente) en sont les conditions nécessaires. Dans le cas contraire, la sécurité ne serait pas suffisante pour activer automatiquement `cupsd`.

12.7.4 Fichiers PPD se trouvant dans différents paquetages

Configuration de l'imprimante avec des fichiers PPD uniquement

Lors de la configuration de l'imprimante avec YaST, les files d'attente de CUPS ne sont créées qu'avec les fichiers PPD installés sur le système correspondant dans `/usr/share/cups/model/`. Pour un modèle d'imprimante particulier, YaST relève les fichiers PPD appropriés en comparant le nom du fabricant et celui du modèle relevé lors de la reconnaissance de matériel avec les noms des fabricants et ceux des modèles dans tous les fichiers PPD présents dans le système dans `/usr/share/cups/model/`. Pour ce faire, la configuration de l'imprimante avec YaST génère une base de données à partir des informations concernant le fabricant et le modèle se trouvant dans les fichiers PPD. Cela vous permet de choisir votre imprimante par le biais des noms de fabricant et de modèle et d'obtenir par conséquent les fichiers PPD correspondant aux noms du fabricant et du modèle.

L'avantage d'une configuration exécutée uniquement à l'aide de fichiers PPD et sans aucune autre source d'informations est que les fichiers PPD sont modifiables à volonté dans `/usr/share/cups/model/`. La configuration de l'imprimante avec YaST relève les modifications et génère à nouveau la base de données comprenant les noms des fabricants et des modèles. Si vous utilisez uniquement des imprimantes PostScript, vous n'avez normalement besoin ni des fichiers PPD Foomatic du paquetage `cups-drivers` ni des fichiers PPD GimpPrint du paquetage `cups-drivers-stp`. Vous pouvez copier les fichiers PPD adaptés exactement à vos imprimantes PostScript dans `/usr/share/cups/model/` (si ceux-ci n'existent pas déjà dans le paquetage `manufacturer-PPDs`) et configurer vos imprimantes de manière optimale.

Fichiers PPD CUPS du paquetage cups

Les fichiers PPD génériques du paquetage `cups` ont été spécialement complétés pour les imprimantes PostScript Niveau 2 et Niveau 1 avec les fichiers PPD Foomatic adaptés suivants :

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

Fichiers PPD du paquetage cups-drivers

Pour les imprimantes non PostScript, on utilise normalement le filtre d'impression Foomatic `foomatic-rip` en même temps que Ghostscript. Les fichiers PPD Foomatic adéquats sont caractérisés par les entrées `*NickName: ... Foomatic/Ghostscript driver` et `*cupsFilter: ... foomatic-rip`. Ces fichiers PPD se trouvent dans le paquetage `cups-drivers`.

YaST utilise de préférence un fichier PPD Foomatic si un fichier PPD avec l'entrée `*NickName: ... Foomatic ... (recommended)` correspond au modèle d'imprimante et s'il n'existe aucun fichier PPD plus adapté dans le paquetage `manufacturer-PPDs` (voir ci-dessous).

Fichiers PPD GimpPrint du paquetage cups-drivers-stp

Pour beaucoup d'imprimantes non PostScript, il est possible d'utiliser comme alternative à `foomatic-rip` le filtre CUPS `rastertoprinter` de GimpPrint. Ce filtre et les fichiers PPD GimpPrint appropriés se trouvent dans le paquetage `cups-drivers-stp`. Les fichiers PPD GimpPrint se trouvent dans `/usr/share/cups/model/stp/` et sont caractérisés par les entrées `*NickName: ... CUPS+Gimp-Print` et `*cupsFilter: ... rastertoprinter`.

Fichiers PPD de fabricants d'imprimantes dans le paquetage manufacturer-PPDs

Le paquetage `manufacturer-PPDs` contient des fichiers PPD de fabricants d'imprimantes couverts par une licence assez libre. Il convient de configurer les imprimantes PostScript avec le fichier PPD adéquat du fabricant d'imprimantes, celui-ci permettant d'utiliser toutes les fonctions de l'imprimante PostScript. YaST utilise de préférence un fichiers PPD du paquetage `manufacturer-PPDs` si les conditions suivantes sont remplies :

- Les noms de fabricant et de modèle déterminés lors de la reconnaissance du matériel correspondent aux noms de fabricant et de modèle dans un fichier PPD du paquetage `manufacturer-PPDs`.
- Le fichier PPD du paquetage `manufacturer-PPDs` est le seul fichier PPD adapté au modèle d'imprimante ou il existe un fichier PPD Foomatic avec l'entrée `*NickName: ... Foomatic/Postscript (recommended)` qui s'adapte également au modèle d'imprimante.

Dans les cas suivants, YaST n'utilise donc aucun fichier PPD du paquetage `manufacturer-PPDs` :

- Le fichier PPD du paquetage `manufacturer-PPDs` ne correspond pas au nom du fabricant et du modèle. Ceci est surtout le cas si, pour des modèles similaires, il n'existe qu'un seul fichier PPD du paquetage `manufacturer-PPDs`, par exemple, si pour une série de modèles, il n'existe pas un fichier PPD pour chaque modèle, mais que le nom de modèle est spécifié sous la forme `Funprinter 1000 series` dans le fichier PPD.
- Le fichier PPD Foomatic Postscript n'est pas recommandé parce que le modèle d'imprimante ne fonctionne pas suffisamment correctement en mode PostScript, par exemple l'imprimante peut fonctionner de manière peu fiable dans ce mode parce qu'elle a trop peu de mémoire ou bien elle est trop lente parce que son processeur n'est pas assez puissant. En outre, l'imprimante peut ne pas prendre en charge PostScript par défaut, par exemple parce que la prise en charge de PostScript n'est disponible que comme module optionnel.

Si, pour ces raisons, il existe un fichier PPD du paquetage `manufacturer-PPDs` correspondant à cette imprimante PostScript que YaST n'est pas à même de configurer, il faut alors choisir à la main dans YaST le modèle d'imprimante adapté.

12.8 Problèmes éventuels et leurs solutions

Les sections suivantes traitent des problèmes matériels et logiciels les plus fréquents en matière d'impression et indiquent des solutions pour résoudre ou contourner ces problèmes.

12.8.1 Imprimante sans prise en charge d'un langage d'impression standard

Une imprimante qui ne prend en charge aucun langage d'impression courant et ne peut être pilotée que par des séquences de contrôle qui lui sont propres s'appelle une *Imprimante GDI*. Ce type d'imprimantes fonctionne uniquement avec des versions du système d'exploitation pour lesquelles le fabricant livre un pilote. *GDI* est une interface de programmation pour la représentation graphique développée par Microsoft. Le problème ne réside pas dans l'interface de programmation mais dans le fait que les imprimantes GDI peuvent uniquement être pilotées au moyen du langage d'impression propriétaire de ce modèle d'imprimante.

Il existe des imprimantes qui, en plus du mode GDI, comprennent un langage d'impression standard. Pour certaines imprimantes GDI, il existe des pilotes propriétaires offerts par le fabricant de l'imprimante. Les pilotes d'impression propriétaires présentent l'inconvénient de ne pouvoir garantir ni leur fonctionnement avec le système d'impression actuellement installé ni leur fonctionnement pour les diverses plateformes matérielles. En revanche, les imprimantes capables de comprendre un langage d'impression standard ne dépendent ni d'une version particulière du système d'impression, ni d'une plateforme matérielle particulière.

Il est en général moins onéreux d'acheter une imprimante prise en charge que de gaspiller du temps à adapter un pilote Linux propriétaire. Avec une imprimante appropriée, le problème lié au pilote est résolu une fois pour toute et vous n'aurez plus à installer ni à configurer un logiciel pilote spécial, ni même à vous procurer des mises à jour du pilote dans le cas où le système d'impression aurait encore évolué.

12.8.2 Pas de fichier PPD adapté à une imprimante PostScript

Si le paquetage `manufacturer-PPDs` ne contient aucun fichier PPD adéquat pour une imprimante PostScript, il devrait être possible d'utiliser le fichier PPD à

partir du CD de pilote du fabricant de l'imprimante ou de télécharger un fichier PPD adapté à partir de la page internet du fabricant de l'imprimante.

Lorsque le fichier PPD se présente en tant qu'archive zip (.zip) ou bien en tant qu'archive zip auto-extractible (`.exe`), vous pouvez le décomprimer avec `unzip`. Informez-vous d'abord sur les conditions de licence du fichier PPD. Vérifiez ensuite au moyen de `cupstestppd` si le fichier PPD correspond à "Adobe PostScript Printer Description File Format Specification, version 4.3.". Si le résultat de l'utilitaire est "FAIL", les erreurs dans les fichiers PPD sont importantes et pourraient causer des problèmes plus conséquents. Il convient d'éliminer les points problématiques indiqués par `cupstestppd`. Si nécessaire, demandez un fichier PPD adéquat directement auprès du fabricant de l'imprimante.

12.8.3 Ports parallèles

La méthode la plus sûre consiste à connecter l'imprimante directement sur le premier port parallèle et de procéder dans le BIOS aux réglages suivants du port parallèle :

- I/O address: `378` (hexadecimal)
- Interrupt: irrelevant
- Mode: `Normal`, `SPP`, or `Output Only`
- DMA: disabled

Si, malgré ces réglages du BIOS, on ne peut pas communiquer avec l'imprimante sur le premier port parallèle, il faut, dans `/etc/modprobe.conf`, saisir, de façon explicite en accord avec les paramètres du BIOS, l'adresse d'entrée-sortie (I/O) sous la forme `0x378`. S'il existe deux ports parallèles réglés sur les adresses I/O `378` et `278` (hexadécimal), il faut les saisir sous la forme `0x378,0x278`.

Si l'interruption `7` est libre, le mode interruption peut être activé par l'entrée montrée dans l'exemple 12.1 de la présente page. Avant d'activer le mode interruption, vérifiez dans le fichier `/proc/interrupts` quelles interruptions sont déjà utilisées. Seules sont affichées les interruptions actuellement utilisées. Ceci peut varier en fonction du matériel actif. L'interruption pour le port parallèle ne doit pas être utilisée par un autre périphérique. En cas de doute, optez pour le mode polling en saisissant `irq=none`.

Example 12.1: */etc/modprobe.conf : mode interruption pour le premier port parallèle*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

12.8.4 Connexions des imprimantes en réseau

Mise en évidence des problèmes de réseau
Connectez l'imprimante directement sur l'ordinateur. Configurez l'imprimante en tant qu'imprimante locale pour effectuer un test. Si l'imprimante fonctionne, le réseau est à l'origine du problème.

Test du réseau TCP/IP Le réseau TCP/IP et la résolution du nom doivent fonctionner correctement.

Test d'un démon `lpd` distant Grâce à la commande suivante, il est possible de vérifier si une connexion TCP au démon `lpd` (port `515`) est possible sur l'ordinateur ⟨*hôte*⟩ :

```
netcat -z host 515 && echo ok || echo failed
```

S'il n'est pas possible de se connecter au démon `lpd`, cela peut signifier que le démon `lpd` ne fonctionne pas ou qu'il existe des problèmes de réseau fondamentaux.

Il est possible de demander, en tant qu'utilisateur `root`, un rapport d'état (éventuellement assez long) sur la file d'attente ⟨*file*⟩ de l'⟨*hôte*⟩ distant à l'aide de la commande suivante, à condition que le démon `lpd` qui s'y trouve fonctionne et qu'il soit possible d'envoyer des requêtes à l'hôte :

```
echo -e ".004<file>" \
  | netcat -w 2 -p 722 <hôte> 515
```

Si `lpd` ne répond pas, cela signifie soit qu'il ne fonctionne pas, soit qu'il existe des problèmes de réseau sous-jacents. Si `lpd` répond, la réponse devrait indiquer la raison pour laquelle il n'est pas possible d'imprimer sur la `file d'attente` de l'`hôte`. Si vous recevez une réponse telle que dans l'exemple 12.2 de la présente page, cela signifie que le problème est causé par le démon `lpd` distant.

***Example 12.2:** Message d'erreur de* `lpd`

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Tester un démon `cupsd` distant Par défaut, le serveur réseau CUPS devrait diffuser ses files d'attente toutes les 30 secondes sur le port UDP `631`. Grâce à la commande suivante, il est donc possible de tester s'il existe un serveur réseau CUPS dans le réseau.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Si un serveur réseau CUPS effectuant une diffusion existe, il devrait apparaître un message tel celui dans l'exemple 12.3 de la présente page.

Example 12.3: *Diffusion à partir du serveur réseau CUPS*

```
ipp://<hôte>.<domaine>:631/printers/<fichier>
```

Grâce à la commande suivante, il est possible de vérifier si une connexion TCP au démon `cupsd` (port `631`) est possible sur l'⟨*hôte*⟩ :

```
netcat -z host 631 && echo ok || echo failed
```

S'il n'est pas possible de se connecter au démon `cupsd`, cela peut signifier que le démon `cupsd` ne fonctionne pas ou qu'il existe des problèmes de réseau fondamentaux. La commande `lpstat -h host -l -t` donne un rapport d'état (éventuellement assez long) sur toutes les files d'attente de l'⟨*hôte*⟩ à condition que le démon `cupsd` qui s'y trouve fonctionne et qu'il soit possible d'envoyer des requêtes à l'hôte.
La commande suivante peut être utilisée pour tester si la file d'attente ⟨*file*⟩ sur l'⟨*hôte*⟩ accepte un travail d'impression qui ne consiste que d'un retour de chariot. Rien ne doit être imprimé. Le cas échéant, une page vide peut être éjectée.

```
echo -en ".r" \
  | lp -d <file> -h <hôte>
```

Recherche d'erreur pour une imprimante réseau ou le boîtier serveur d'impression
Le spouleur qui fonctionne dans un boîtier serveur d'impression pose parfois problème dès que la quantité des requêtes d'impression est élevée. Étant donné que le spouleur du boîtier serveur d'impression est à l'origine des problèmes, on ne peut rien y faire. Il est cependant possible de contourner le spouleur du boîtier serveur d'impression en pilotant directement via

socket TCP l'imprimante connectée au boîtier serveur d'impression. Voir la section 12.5.2 page 269.

Par conséquent, le boîtier serveur d'impression ne fait plus qu'office de convertisseur entre les différentes formes de transmission de données (réseau TCP/IP et connexion d'imprimante locale), ce qui signifie que le port TCP correspondant sur le boîtier serveur d'impression doit être connu. Lorsque l'imprimante est connectée et allumée sur le boîtier serveur d'impression, il est normalement possible de relever ce port TCP au moyen de `nmap` du paquetage `nmap` un laps de temps après avoir allumé le boîtier serveur d'impression . Par exemple, pour un boîtier serveur d'impression, la commande `nmap` ⟨*adresse IP*⟩ peut donner :

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

Cet affichage signifie que l'imprimante connectée au boîtier serveur d'impression peut être commandée par socket TCP sur le port `9100`. Par défaut, `nmap` n'examine qu'une certaine liste de ports bien connus, listés dans `/usr/share/nmap/nmap-services`. Afin d'examiner tous les ports possibles, utilisez la commande `nmap -p` ⟨*from_port*⟩-⟨*to_port*⟩ ⟨*IP-address*⟩. Ceci peut prendre un peu de temps. Pour plus d'informations, consultez la page de manuel de `nmap`.

Entrez une commande telle que

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

pour envoyer directement des chaînes de caractères ou des données au port correspondant pour tester si l'imprimante peut être adressée sur ce port.

12.8.5 Impressions défectueuses sans message d'erreur

Le système d'impression considère le travail d'impression comme entièrement achevé lorsque le backend CUPS a terminé la transmission des données vers le destinataire (l'imprimante). Si par la suite le destinataire ne réussit pas à effectuer le traitement requis, par exemple, si l'imprimante n'arrive pas à sortir sur

papier les données qui lui sont destinées, le système d'impression ne s'en rend pas compte. Si l'imprimante n'arrive pas à imprimer sur papier les données qui lui sont destinées, il faut alors choisir un autre fichier PPD mieux adapté à l'imprimante.

12.8.6 Files d'attente désactivées

Lorsque la transmission des données au récepteur a totalement échoué après plusieurs essais, le backend de CUPS, par exemple `usb` ou `socket`, signale une erreur au système d'impression (au démon `cupsd`). Le backend décide s'il convient d'entreprendre d'autres essais ainsi que le nombre d'essais avant de signaler qu'il est impossible de transmettre les données. Comme d'autres essais ne sont pas utiles, `cupsd` désactive alors l'impression sur la file d'attente concernée. Après avoir éliminé l'origine du problème, l'administrateur système doit réactiver l'impression à l'aide de la commande `/usr/bin/enable`.

12.8.7 Diffusion CUPS : effacer des travaux d'impression

Lorsqu'un serveur réseau CUPS diffuse ses files d'attente aux hôtes clients et qu'un démon `cupsd` local adéquat est actif sur les ordinateurs clients, c'est le démon `cupsd` du client qui accepte les travaux d'impression des applications pour les remettre immédiatement au démon `cupsd` du serveur. Lorsqu'un démon `cupsd` accepte une requête d'impression, il lui est conféré un nouveau numéro d'impression. C'est la raison pour laquelle le numéro d'impression sur l'hôte client est différent du numéro sur le serveur. Étant donné qu'un travail d'impression est immédiatement remis, il ne peut pas être annulé sous le numéro de l'ordinateur client parce que le démon `cupsd` du client considère la requête d'impression comme totalement achevée dès qu'il l'a transmise au `cupsd` du serveur.

Pour annuler une requête d'impression sur le serveur, il faut saisir une commande telle que `lpstat -h <serveur impression> -o`pour relever le numéro d'impression sur le serveur à condition que le serveur n'ait pas terminé la requête d'impression (c'est-à-dire envoyé à l'imprimante). Il est ensuite possible d'annuler le travail d'impression sur le serveur :

```
cancel -h <serveur impression> <fichier>-<numéro travail>
```

12.8.8 Travaux d'impression defectueux et erreurs lors du transfert de données

Si vous éteignez et réallumez l'imprimante ou l'ordinateur pendant la procédure d'impression, les travaux restent tout de même dans les files d'attente et seront réimprimées à partir du début. Vous devez supprimer un travail d'impression défectueux de la file d'attente à l'aide de la commande `cancel`.

Si un travail d'impression est défectueux ou si la communication entre l'ordinateur et l'imprimante est perturbée, l'imprimante n'est plus à même de traiter correctement les données, entraînant l'impression d'une quantité de feuilles couvertes de caractères confus.

1. Pour arrêter l'impression, sortez d'abord tout le papier dans le cas d'imprimantes à jet d'encre ou bien ouvrez les cassettes de papier dans le cas d'imprimantes laser. Les imprimantes haut de gamme sont souvent dotées d'un bouton sevant à stopper l'impression en cours.
2. Étant donné que le travail d'impression n'est retiré de la file d'attente qu'après avoir été envoyé à l'imprimante, il devrait normalement rester dans la file d'attente. Entrez `lpstat -o` ou `lpstat -h` ⟨*serveur d'impression*⟩ `-o` pour savoir à partir de quelle file d'attente l'impression est effectuée. Annulez le travail d'impression en saisissant `cancel` ⟨*file d'attente*⟩-⟨*numéro d'impression*⟩ ou `cancel -h` ⟨*serveur d'impression*⟩ ⟨*file d'attente*⟩-⟨*numéro d'impression*⟩ .
3. Il est possible que, bien que le travail d'impression ait été retiré de la file d'attente, quelques données soient encore transmises à l'imprimante. Contrôlez si, pour la file d'attente concernée, un processus backend CUPS est encore en cours et mettez-y fin si nécessaire. Dans le cas d'une imprimante connectée au port parallèle, on peut terminer tous les processus qui accèdent encore à l'imprimante (plus exactement, au port parallèle) au moyen de la commande `fuser -k /dev/lp0`.
4. Désactivez complètement l'imprimante en l'éteignant pendant un certain laps de temps. Puis réalimentez-la en papier et rallumez-la.

12.8.9 Débogage du système d'impression CUPS

Pour analyser les problèmes d'impression avec CUPS, nous recommandons la méthode suivante :

1. Déclarez `LogLevel debug` dans `/etc/cups/cupsd.conf`.
2. Arrêtez le démon `cupsd`.
3. Déplacez `/var/log/cups/error_log*` afin de ne pas avoir à faire une recherche dans des fichiers journaux trop volumineux.
4. Démarrez le démon `cupsd`.
5. Répétez l'opération qui a provoqué le problème.
6. Vous trouverez ensuite des messages dans `/var/log/cups/error_log*` qui vous aideront à trouver l'origine du problème.

12.8.10 Informations complémentaires

De nombreux cas particuliers ont leurs solutions dans la base de données Support. Pour les problèmes d'imprimante, les articles *Installing a Printer* (en anglais), *Installer une imprimante sous SUSE LINUX 9.1* (en français et *Printer Configuration from SUSE LINUX 9.2* (en anglais) qu'elle contient vous seront certainement très utiles ; vous les trouverez en utilisant les mots-clés ″printer“ ou ″imprimante“.

13

Informatique nomade sous Linux

Ce chapitre donne une vue d'ensemble des divers aspects de l'informatique nomade sous Linux. Les différents champs d'application sont brièvement présentés, et les caractéristiques principales du matériel utilisé sont décrites. Le chapitre couvre aussi les solutions logicielles répondant à des besoins spécifiques et les options permettant des performances maximales, ainsi que les possibilités de minimiser la consommation d'énergie. Une vue d'ensemble des sources d'informations les plus conséquentes sur ce sujet conclut le chapitre.

La plupart des gens associe l'informatique nomade aux ordinateurs portables, assistants personnels et téléphones portables et à l'échange de données entre ces appareils. Ce chapitre élargit cette notion aux composants matériels mobiles tels que disques durs externes, cartes mémoire ou appareils photo numériques qui peuvent être connectés à des ordinateurs portables ou à des ordinateurs de bureau.

13.1 Ordinateurs portables

The hardware of laptops differs from that of a normal desktop system. This is because criteria like exchangeability, occupied space, and power consumption are relevant properties. The manufacturers of mobile hardware have developed the PCMCIA standard (*Personal Computer Memory Card International Association*). This standard covers memory cards, network interface cards, ISDN and modem cards, and external hard disks. How the support for such hardware is implemented in Linux, what needs to be taken into account during configuration, what software is available for the control of PCMCIA, and how to troubleshoot any possible problems is described in chapitre 14 page 299.

13.1.1 Économies d'énergie

Le choix de composants système à faible consommation d'énergie lors de la fabrication d'un ordinateur portable est un facteur contribuant à l'adéquation des ordinateurs portables pour une utilisation sans accès au réseau d'alimentation électrique. La contribution de ces composants à l'économie d'énergie est au moins aussi importante que celle de votre système d'exploitation. SUSE LINUX prend en charge différentes méthodes influençant la consommation d'énergie de votre ordinateur portable, qui ont des répercussions plus ou moins importantes sur l'autonomie de la batterie. La liste suivante est classée selon les contributions décroissantes à l'économie d'énergie :

- Réguler la fréquence du processeur
- Arrêter l'éclairage de l'écran dans les phases d'inactivité
- Diminuer manuellement l'éclairage de l'écran
- Déconnecter les périphériques branchés à chaud non utilisés (CDROM USB, souris externe, cartes PCMCIA non utilisées, etc.)
- Arrêter le disque dur lorsqu'il n'est pas actif

Vous trouverez au chapitre chapitre 16 page 321 des informations de fond détaillées concernant la gestion de l'énergie sous SUSE LINUX et l'utilisation du module de gestion d'énergie de YaST.

13.1.2 Intégration dans des environnements d'exploitation changeants

En utilisation nomade, votre système doit s'intégrer à des environnements d'exploitation variables. Beaucoup de services dépendent de l'environnement, et la configuration des clients sous-jacents doit être modifiée. SUSE LINUX prend en charge cette tâche pour vous.

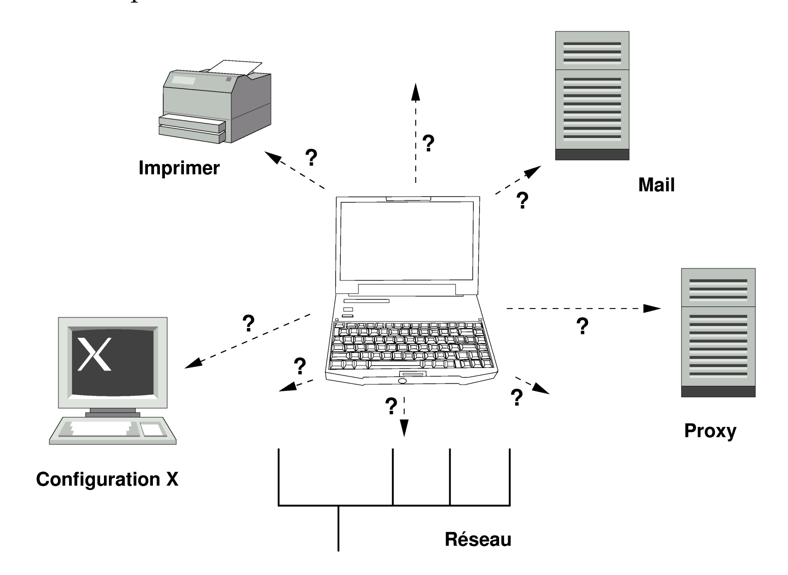


FIG. 13.1: *Intégration d'un ordinateur portable dans un réseau*

Dans le cas d'un ordinateur portable faisant la navette entre un petit réseau domestique et un réseau d'entreprise, les services concernés sont :

Configuration du réseau Cela comprend l'attribution d'une adresse IP, la résolution de noms, la connexion à Internet et la connexion à d'autres réseaux.

Impression Selon le réseau, une base de données actualisée des imprimantes disponibles et un serveur d'impression disponible doivent être présents.

Courrier électronique et serveurs mandataires
Comme pour l'impression, la liste des serveurs concernés doit être à jour.

Configuration de X Si vous connectez temporairement votre ordinateur portable avec un vidéoprojecteur ou un écran externe, les différentes configurations de l'écran doivent être conservées.

SUSE LINUX vous offre deux possibilités (combinables) d'intégrer un ordinateur portable à des environnements d'exploitation existants :

SCPM SCPM (System Configuration Profile Management) vous permet d'enregistrer tout état de configuration du système dans une sorte de "photographie instantanée" appelée *Profil*. On peut créer des profils pour les situations les plus diverses. Ils sont adaptés si le système est utilisé dans des environnements variables (réseau domestique ou réseau d'entreprise). Il est possible de commuter à tout moment entre les différents profils. Vous trouverez des informations sur SCPM dans le chapitre chapitre 15 page 309. Sous KDE, vous pouvez commuter entre profils via l'applet Kicker Profile Chooser . Cette application a besoin du mot de passe de root avant tout changement de profil.

SLP Le Service Location Protocol (en abrégé : SLP) simplifie la connexion d'un ordinateur portable sur un réseau existant. Sans SLP, l'administrateur d'un ordinateur portable a généralement besoin d'informations extensives sur les services disponibles sur le réseau. SLP diffuse à tous les clients d'un réseau local les informations de disponibilité d'un type de service donné. Les applications prenant en charge SLP peuvent utiliser les informations diffusées par SLP et être ainsi automatiquement configurées. SLP peut même être utilisé pour l'installation d'un système sans que vous ayez à vous donner la peine de rechercher une source d'installation adéquate. Vous trouverez des informations détaillées sur SLP à la section chapitre 23 page 459.

L'atout de SCPM est sa capacité à permettre et à maintenir des conditions système qui peuvent être reproduites, tandis que SLP facilite largement la configuration d'un ordinateur en réseau en automatisant une grande partie de cette tâche.

13.1.3 Options logicielles

Dans une utilisation nomade, plusieurs tâches spécifiques sont traitées par des logiciels dédiés : surveillance du système (en particulier l'état de charge de la batterie), synchronisation des données et communication sans fil avec des périphériques et avec Internet. Les sections suivantes présentent pour chaque point les applications les plus importantes fournies par SUSE LINUX.

Surveillance du système

SUSE LINUX propose deux outils KDE destinés à la surveillance du système. Le simple affichage d'état de la batterie de l'ordinateur portable est géré par l'applet KPowersave dans Kicker. KSysguard réalise la surveillance complexe du système. Sous GNOME, les fonctions décrites vous sont proposées par GNOME ACPI (en tant qu'applet du tableau de bord) et System Monitor.

KPowersave KPowersave est une applet qui indique l'état de charge de la batterie dans le panneau de contrôle. L'icône s'adapte pour représenter le type d'alimentation en courant. Lorsque l'ordinateur est relié au réseau électrique, vous voyez une petite icône en forme de prise. Lorsque l'ordinateur fonctionne sur batterie, l'icône est remplacée par une pile. Le menu correspondant ouvre le module de YaST de gestion d'énergie, après que vous ayez fourni le mot de passe de root. Ce module vous permet de configurer le fonctionnement du système dans différentes conditions d'alimentation électrique. Vous trouverez des informations sur la gestion de l'énergie et le module correspondant de YaST dans le chapitre chapitre 16 page 321.

KSysguard KSysguard est une application autonome, qui regroupe tous les paramètres mesurables du système dans un unique environnement de surveillance. KSysguard possède des écrans de contrôle pour ACPI (état de la batterie), la charge du processeur, le réseau, l'état des partitions disque et l'utilisation de la mémoire. Il peut en plus surveiller et afficher l'ensemble des processus système. Vous pouvez régler vous-même la présentation et le filtrage des données collectées. Vous pouvez surveiller différents paramètres système dans des fenêtres séparées ou collecter en parallèle les données de plusieurs ordinateurs par l'intermédiaire du réseau. KSysguard peut également fonctionner comme démon sur les ordinateurs ne possédant pas d'environnement KDE. Vous trouverez plus d'informations sur ce programme grâce à sa fonction d'aide intégrée ou via l'aide en ligne de SUSE.

Synchronisation des données

Si vous passez d'un ordinateur portable non connecté au réseau à une station de travail en réseau sur votre lieu de travail, il est nécessaire de maintenir la synchronisation des données traitées entre les différentes instances. Ceci peut inclure les dossiers de courrier électronique, les répertoires et fichiers individuels dont vous avez besoin tant pour le travail nomade qu'à votre bureau. Une solution pour ces deux situations se présente ainsi :

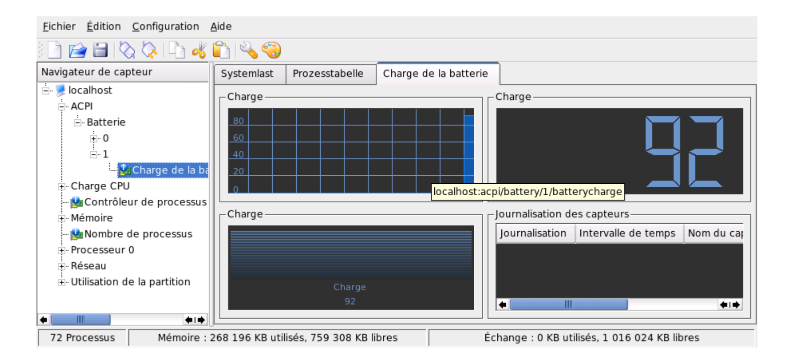


FIG. 13.2: *Surveillance de l'état de charge de la batterie avec KSysguard*

Synchronisation des messages électroniques
Dans le réseau d'entreprise, utilisez un compte IMAP pour enregistrer vos messages électroniques. Depuis votre station de travail, vous pouvez alors lire vos messages avec tout client de messagerie prenant en charge le mode IMAP déconnecté (par exemple Mozilla Thunderbird Mail, Evolution ou KMail, comme décrit dans le *Guide de l'utilisateur*). Le logiciel de messagerie doit être configuré de façon à ce que le dossier utilisé pour `Messages envoyés` soit toujours le même. Ceci garantit que tous les messages sont disponibles, avec leurs informations d'état, une fois que le processus de synchronisation est terminé. Pour l'envoi de messages, utilisez le service SMTP contenu dans le logiciel de messagerie plutôt qu'un agent de transfert de messages au niveau du système (postfix ou sendmail) afin de recevoir une information fiable concernant les messages qui n'ont pas été envoyés.

Synchronisation de fichiers et de répertoires
Il existe plusieurs outils adaptés à la synchronisation de données entre un ordinateur portable et une station de travail. Pour des informations détaillées, reportez-vous à la section chapitre 31 page 569.

Communication sans fil

Un ordinateur portable peut se connecter sans fil à d'autres ordinateurs, périphériques, téléphones portables ou assistant personnel aussi bien qu'à un réseau câblé domestique ou d'entreprise. Linux prend en charge trois types de communications sans fil :

WLAN WLAN, couvrant le plus large éventail de ces technologies sans fil, est le seul à pouvoir être utilisé pour l'exploitation de réseaux de grandes dimensions et même parfois physiquement séparés. Des ordinateurs individuels peuvent se connecter entre eux pour former un réseau autonome sans fil ou pour être connectés à Internet. Des appareils, désignés sous le nom de points d'accès, jouent le rôle de station de base pour les ordinateurs utilisant WLAN et leur permettent, en qualité d'intermédiaire, l'accès à Internet. L'utilisateur nomade peut passer d'un point d'accès à l'autre avec son ordinateur compatible WLAN, selon l'endroit où il se trouve et le point d'accès offrant la meilleure connexion. Comme pour la téléphonie mobile, un utilisateur WLAN dispose d'un large réseau dans lequel il n'est pas contraint à un emplacement spécifique pour pouvoir se connecter. Vous trouverez des détails concernant WLAN dans le chapitre section 17.1 page 348.

Bluetooth Bluetooth dispose du plus large spectre d'utilisation de toutes les technologies sans fil. Comme IrDA, il peut être utilisé pour la communication entre ordinateurs (portables) et assistants personnels ou téléphones portables. Il peut aussi être utilisé pour mettre en réseau plusieurs ordinateurs qui se trouvent à portée de vue l'un de l'autre. Bluetooth est en outre utilisé pour relier des composants système sans fil comme les claviers ou les souris. La portée de cette technologie n'est cependant pas suffisante pour mettre en réseau des systèmes physiquement séparés. WLAN est une technologie plus adaptée pour une communication sans fil à travers des obstacles physiques tels que des murs. Vous trouverez plus d'informations sur Bluetooth, ses applications et sa configuration dans le chapitre section 17.2 page 357.

IrDA IrDA est la technologie sans fil ayant la plus petite portée. Les deux partenaires de communication doivent se trouver à porter de vue l'un de l'autre. Les obstacles tels que les murs sont infranchissables. Une utilisation possible d'IrDA est la transmission d'un fichier depuis un ordinateur portable vers un téléphone portable. La courte distance entre l'ordinateur portable et le téléphone portable est alors couverte par via IrDA. Le transport sur une longue distance jusqu'au destinataire du fichier est réalisé par l'intermédiaire du réseau de téléphonie mobile. Une autre application d'IrDA est l'envoi sans fil de requêtes d'impression au bureau. Vous trouverez plus d'informations sur IrDA au chapitre section 17.3 page 369.

13.1.4 Sécurité des données

Idéalement, vous devez sécuriser vos données sur votre ordinateur portable contre un accès non autorisé, et ce de plusieurs façons. Des mesures de sécurité peuvent être prises dans les domaines suivants :

Protection contre le vol Vous devez toujours, dans la mesure du possible, assurer la sécurité physique de votre système contre le vol. Différents systèmes de sécurité sont disponibles dans le commerce (comme par exemple des câbles antivol).

Sécurisation des données dans le système
Les données importantes doivent non seulement être chiffrées lors d'une transmission, mais aussi sur le disque dur de votre système. La création d'une partition chiffrée avec SUSE LINUX est décrite dans la section section 34.3 page 646.

Sécurité du réseau Tout échange de données doit être sécurisé, quelle que soit la façon dont il a lieu. Les aspects généraux de sécurité sous Linux et en réseau sont traités au chapitre section 34.4 page 649. Des mesures de sécurité concernant les réseaux sans fil vous sont proposées au chapitre chapitre 17 page 347.

13.2 Matériel mobile

SUSE LINUX prend en charge la reconnaissance automatique de périphériques de stockage amovibles via Firewire (IEEE 1394) ou USB. On entend par "périphériques de stockage amovibles" tous les types de disques durs Firewire ou USB, cartes mémoire USB ou appareils photo numériques. Dès que ces périphériques sont reliés au système par l'interface correspondante, ils sont automatiquement reconnus et configurés par hotplug. subfs et submount veillent à ce que les périphériques soient montés aux emplacements appropriés dans le système de fichiers. Cette procédure épargne entièrement à l'utilisateur le montage et le démontage manuel en vigueur dans les précédentes versions de SUSE LINUX. Dès que le périphérique n'est plus utilisé par aucun programme, vous pouvez simplement le déconnecter.

Disques durs externes (USB et Firewire)
Dès qu'un disque dur externe a été correctement reconnu par le système, vous pouvez voir apparaître son icône dans 'Mon ordinateur' (KDE) ou

'Ordinateur' (GNOME) dans la vue d'ensemble des lecteurs montés. Si vous cliquez avec le bouton gauche de la souris sur l'icône, le contenu du lecteur apparaît. Vous pouvez à cet endroit créer des fichiers ou des dossiers, les modifier ou les effacer. Si vous désirer renommer le disque dur d'une autre manière que le nom donné par le système, cliquez avec le bouton droit de la souris sur l'icône et choisissez l'entrée de menu correspondante. Cette modification du nom se limite cependant à l'affichage dans le gestionnaire de fichiers. La désignation sous laquelle le périphérique est monté dans `/media/usb-xxx` ou `/media/ieee1394-xxx` reste inchangée.

Cartes mémoires USB Ces périphériques sont considérés par le système exactement comme des disques durs externes. Il est également possible de les renommer dans le gestionnaire de fichiers.

Appareils photo numériques (USB et Firewire)
Les appareils photo numériques reconnus par le système apparaissent aussi en tant que lecteurs externes dans la vue d'ensemble du gestionnaire de fichiers. Sous KDE, vous pouvez lire et regarder les photographies par l'intermédiaire de l'URL `camera:/`. Utilisez digikam ou The Gimp pour travailler sur les images. Sous GNOME, les images sont affichées dans Nautilus dans leur dossier respectif. GThumb est un utilitaire simple de traitement et de gestion des images. A l'exception de GThumb, tous les programmes mentionnés sont décrits dans le *Guide de l'utilisateur*. Vous y trouverez également un chapitre sur les appareils photos numériques.

Important

Assurer la sécurité des supports de données mobiles

Tout comme les ordinateurs portables, les disques durs prévus pour le voyage ou les cartes mémoire ne sont pas à l'abri des vols. Afin d'empêcher un usage abusif des données s'y trouvant, il est conseillé de créer une partition chiffrée, comme décrit dans la section section 34.3 page 646.

Important

13.3 Téléphones portables et assistants personnels

Un ordinateur de bureau ou un ordinateur portable peut communiquer avec un téléphone portable via Bluetooth ou via IrDA. Quelques modèles prennent en charge les deux protocoles, certains n'en gèrent qu'un seul. Les domaines d'utilisation des deux protocoles et la documentation supplémentaire s'y rapportant ont déjà été mentionnés à la section section Communication sans fil page 292. Vous trouverez dans la documentation du téléphone portable comment configurer ces protocoles sur le téléphone même. Vous trouverez la description de la configuration côté Linux aux sections section 17.2 page 357 et section 17.3 page 369.

La prise en charge de la synchronisation avec des assistants personnels fabriqués par Palm est déjà intégrée dans Evolution et Kontact. La connexion initiale avec l'assistant personnel est, dans les deux cas, facile à réaliser avec l'aide d'un programme assistant. Une fois la prise en charge du Palm Pilot configurée, définissez quels types de données vous voulez synchroniser (adresses, rendez-vous, etc...). Les deux programmes de travail collaboratif sont décrits dans le *Guide de l'utilisateur*.

Le programme KPilot intégré dans Kontact est également disponible en tant que programme autonome. Vous en trouverez une description dans le *Guide de l'utilisateur*. Il existe également le programme KitchenSync pour la synchronisation de données d'adresses.

Pour plus informations sur Evolution et Kontact, veuillez consulter le *Guide de l'utilisateur*.

13.4 Pour plus d'informations

La référence centrale pour toutes les questions concernant les périphériques mobiles sous Linux est `http://tuxmobil.org/`. Plusieurs sections de ce site internet traitent des aspects matériels et logiciels concernant les ordinateurs portables, assistants personnels, téléphones portables et autres matériels mobiles.

`http://www.linux-on-laptops.com/` possède une approche similaire à celle de `http://tuxmobil.org/`. Vous y trouverez des informations sur les ordinateurs portables et les assistants personnels.

SUSE dispose d'un liste de diffusion dédiée aux ordinateurs portables (en allemand) : `http://lists.suse.com/archive/suse-laptop/`. Des utilisateurs et développeurs y discutent de tous les aspects du travail nomade sous SUSE LINUX. On y répond aux messages en anglais, mais la majeure partie des informations archivées est disponible exclusivement en allemand.

En cas de problèmes avec la gestion de l'énergie sur les ordinateurs portables sous SUSE LINUX, il est recommandé de jeter un oeil sur les fichiers `README` sous `/usr/share/doc/packages/powersave`. Ce répertoire contient souvent les derniers retours d'expérience de testeurs et développeurs si bien qu'il fournit souvent des indications précieuses pour la résolution de vos problèmes.

PCMCIA

Ce chapitre traite des particularités des ordinateurs portables et plus particulièrement des apects matériels et logiciels de PCMCIA. PCMCIA signifie, en anglais, *Personal Computer Memory Card International Association* est un terme générique qui désigne tous les logiciels et tout le matériel informatique de ce type.

14.1 Matériel

Le composant essentiel est la carte PCMCIA dont on distingue deux types :

Cartes PC Ces carte existent depuis les premiers jours de PCMCIA. Elles utilisent un bus de 16 bits pour le transfert des données et sont relativement économiques. Certains ponts PCMCIA modernes ont du mal à reconnaître ces cartes. Cependant, une fois reconnues, elles sont, en règle générale, prises en charge sans problème et de manière stable.

Cartes CardBus Il s'agit d'un nouveau standard de cartes. Elles utilisent un bus de 32 bits, et sont donc plus rapides mais aussi plus chères. Elles sont connectés au système comme des cartes PCI et sont donc utilisables sans problème.

Pour savoir quelle carte vous utilisez, lorsque le service PCMCIA est actif, saisissez la commande `cardctl ident` . Vous trouverez une liste des cartes prises en charge dans le fichier `SUPPORTED.CARDS` dans le répertoire `/usr/share/doc/packages/pcmcia`. Vous y trouverez aussi la version actuelle du HOWTO PCMCIA.

Le deuxième composant indispensable est le contrôleur PCMCIA ou également la carte PC ou le pont CardBus. Celui-ci assure la connexion entre la carte et le bus PCI. Tous les modèles courants sont pris en charge. Utilisez la commande `pcic_probe` pour déterminer le type du contrôleur. S'il s'agit d'un appareil PCI, la commande `lspci -vt` permet aussi d'obtenir des informations intéressantes.

14.2 Logiciels

Les sections suivantes traitent des aspects logiciels de PCMCIA. Vous apprendrez ici des détails relatifs aux modules noyau impliqués et au gestionnaire de cartes.

14.2.1 Modules de base

Les modules du noyau nécessaires se trouvent dans les paquetages du noyau. Vous avez, en outre, besoin des paquetages `pcmcia` et `hotplug`. Lors du démarrage de PCMCIA, les modules `pcmcia_core`, `yenta_socket` et `ds` sont chargés. Dans quelques rares cas, le module `tcic` est nécessaire à la place de `yenta_socket`. Ces modules permettent d'initialiser les contrôleurs PCMCIA disponibles et proposent des fonctionnalités de base.

14.2.2 Gestionnaire de cartes

Comme les cartes PCMCIA peuvent être changées pendant le fonctionnement de l'ordinateur, les activités au niveau des emplacements doivent être surveillées. Cette tâche est effectuée par les *Services cartes* implémentés dans le modules de base. L'initialisation d'une carte insérée est faite soit par le *gestionnaire de cartes* (pour cartes PC), soit par le système hotplug du noyau (pour les cartes CardBus). Le gestionnaire de cartes est démarré à l'aide du script de démarrage PCMCIA après le chargement des modules de base. Hotplug est automatiquement activé.

Lors de l'insertion d'une carte, le gestionnaire de cartes ou la connexion hotplug établit son type et sa fonction et charge les modules adaptés. Si ces derniers sont correctement chargés, le gestionnaire de cartes ou la connexion hotplug, selon la fonction de la carte, démarrent des scripts d'initialisation particuliers qui établissent la connexion réseau de leur côté, montent des partitions de disques SCSI externes ou effectuent d'autres actions propres au matériel. Les scripts du gestionnaire de cartes se trouvent dans `/etc/pcmcia`. Les scripts de connexion hotplug se trouvent dans `/etc/hotplug`. Lorsque la carte est à nouveau retirée, le gestionnaire de cartes ou la connexion hotplug utilisent les mêmes scripts pour mettre un terme aux diverses activités relatives aux cartes. Enfin, les modules devenus inutiles sont à nouveau déchargés.

Pour des processus de ce type, il existe des événements "hotplug". Lorsque des disques durs ou des partitions sont ajoutés (événements ”block“), les scripts hotplug veillent à ce que les nouveaux supports de données soient immédiatement disponibles dans `/media` à travers `subfs`. Pour monter des supports de données à travers les anciens scripts PCMCIA, Hotplug doit être désactivé dans `subfs`.

Aussi bien le processus de démarrage de PCMCIA que les événements relatifs aux cartes sont enregistrés dans le journal du système (`/var/log/messages`). Les modules qui sont chargés et les scripts qui sont exécutés pour la configuration y sont précisés.

Théoriquement, une carte PCMCIA peut être retirée simplement. Cela fonctionne également particulièrement bien pour les cartes réseau, modem ou RNIS, en l'absence de connexion réseau encore active. Cela ne fonctionne en revanche pas pour ce qui concerne les partitions montées d'un disque dur externe ou les répertoires NFS. Vous devez, pour ce faire, veiller à ce que les unités soient synchronisées et démontées proprement. Cela n'est naturellement plus possible si la carte a déjà été retirée. En cas de doute, n'hésitez pas à utiliser la commande `cardctl eject`. Cette commande permet de désactiver toutes les cartes qui se trouvent toujours dans le portable. Pour ne désactiver qu'une seule des cartes, vous pouvez aussi indiquer son numéro d'emplacement, par exemple, `cardctl eject 0`.

14.3 Configuration

Pour définir si PCMCIA doit démarrer lors de l'amorçage, utilisez l'éditeur de niveaux d'exécution de YaST. Démarrez ce module avec 'Système' → 'Éditeur de niveaux d'exécution'.

Les trois variables suivantes sont définies dans le fichier `/etc/sysconfig/pcmcia` :

`PCMCIA_PCIC` contient le nom du module piloté par le contrôleur PCMCIA. Normalement, le script de démarrage détermine ce nom tout seul. Ce n'est qu'en cas d'échec que le module doit être enregistré ici. Sinon cette variable doit rester vide.

`PCMCIA_CORE_OPTS` est prévu pour les paramètres du module `pcmcia_core` ; ils ne sont cependant que très rarement utilisés. Ces options sont décrites dans la page de manuel de pcmcia_core(4). Étant donné que cette page de manuel fait référence au module de même nom que le paquetage `pcmcia-cs` de David Hinds, elle contient plus de paramètres que n'en propose réellement le module du noyau, c'est à dire tous ceux qui commencent par `cb_` et `pc_debug`.

`PCMCIA_BEEP` allume et éteint les signaux acoustiques du gestionnaire de cartes.

L'attribution des pilotes aux cartes PCMCIA pour le gestionnaire de cartes se trouve dans les fichiers `/etc/pcmcia/config` et `/etc/pcmcia/*.conf`. `config` est d'abord lu, puis `*.conf` dans l'ordre alphabétique. C'est le dernier élément trouvé pour une carte qui est utilisé. Vous trouverez des détails sur la syntaxe de ces fichiers sur la page de manuel relative de pcmcia(5).

L'attribution des pilotes aux cartes CardBus se fait dans les fichiers `/etc/sysconfig/hardware/hwcfg-<nomconfiguration>`. Ces fichiers sont créés par YaST lors de la configuration d'une carte. Vous trouverez plus de détails sur les noms de configuration sous `/usr/share/doc/packages/sysconfig/README` et dans la page de manuel de getcfg(8).

14.3.1 Cartes réseau

À l'instar des cartes réseau ordinaires, vous pouvez installer les cartes réseaux Ethernet, Wireless LAN et TokenRing avec YaST. Si votre carte n'est pas reconnue, vous ne devez que préciser comme type de carte, `PCMCIA`, lors de la configuration du matériel. Tous les autres détails relatifs à la mise en place du réseau sont décrits dans la section 22.4 page 433.

14.3.2 RNIS

Vous pouvez aussi configurer les cartes PC RNIS comme des cartes RNIS ordinaires avec YaST. Peu importe laquelle des cartes RNIS PCMCIA proposées vous choisissez : la seule chose importante est qu'il s'agisse bien d'une carte PCMCIA. Lors de la configuration du matériel et de la sélection du fournisseur d'accès, il faut veiller à ce que le mode de fonctionnement soit toujours `hotplug`, et pas `onboot`. Il existe aussi des modems RNIS dans les cartes PCMCIA. Il s'agit de cartes modem ou multifonctions avec un kit de connexion RNIS supplémentaire. Elles sont traitées comme un modem.

14.3.3 Modem

Les cartes PC modem ne disposent normalement d'aucun réglage spécifique PCMCIA. Dès qu'une carte modem est insérée, elle est disponible dans `/dev/modem`. Il existe aussi pour les cartes PCMCIA ce que l'on appelle des modems logiciels. Ils ne sont généralement pas pris en charge. S'il existe des pilotes pour ces derniers, vous devrez les intégrer individuellement au système.

14.3.4 SCSI et IDE

Le module de pilotes adapté est chargé par le gestionnaire de cartes ou la connexion hotplug. Ainsi, dès l'insertion d'une carte SCSI ou IDE, les appareils qui y sont connectés sont disponibles. Les noms des appareils sont déterminés de manière dynamique. Vous trouverez des informations sur les appareils SCSI ou IDE dans `/proc/scsi` ou dans `/proc/ide`.

Les disques durs, les lecteurs de CD-ROM et autres appareils externes de ce type doivent être éteints avant d'insérer la carte PCMCIA dans son emplacement. Les appareils SCSI doivent être arrêtés de manière active.

Avertissement

Retrait d'une carte SCSI ou IDE

Avant de retirer une carte SCSI ou IDE, il faut démonter toutes les partitions des appareils qui y sont connectés (avec la commande `umount`). Si vous oubliez de le faire, vous ne pourrez à nouveau accéder à ces appareils qu'après un redémarrage du système.

Avertissement

14.4 Utilitaires

Le programme cité ci-avant, cardctl, est l'outil pour obtenir des informations sur PCMCIA ou exécuter certaines actions. Vous trouverez des détails dans la page de manuel de cardctl(8). Après la saisie de `cardctl`, vous obtenez une liste des options disponibles. Il existe également un frontal graphique pour ce programme, cardinfo, avec lequel les choses les plus importantes sont contrôlables. Pour cela le paquetage `pcmcia-cardinfo` doit être installé.

`ifport`, `ifuser`, `probe` et `rcpcmcia` du paquetage `pcmcia` vous apporteront également de l'aide. Cependant, ils ne sont pas toujours nécessaires.

Pour savoir exactement quels fichiers sont contenus dans le paquetage `pcmcia`, utilisez la commande `rpm -ql pcmcia`.

14.5 Problèmes possibles et solutions

En cas de problèmes avec PCMCIA sur certains ordinateurs portables ou avec certaines cartes, vous réglerez la plupart de ces difficultés assez facilement, dans la mesure où vous traiterez toujours le problème de manière systématique. Tout d'abord, il faut déterminer si le problème vient de la carte ou s'il s'agit d'un problème au niveau du système de base PCMCIA. Vous devez donc, dans tous les cas, commencer par démarrer l'ordinateur sans que la carte ne soit insérée. Ce n'est que quand le système de base fonctionnera apparemment sans problème que vous pourrez réinsérer la carte. Tous les messages sont enregistrés dans le fichier journal `/var/log/messages`. Vous devez donc particulièrement surveiller ce fichier avec `tail -f /var/log/messages` pendant les tests. Ainsi l'erreur se limite à l'un des deux cas suivants.

14.5.1 Le système de base PCMCIA ne fonctionne pas

Lorsque le système reste bloqué lors de l'amorçage dès le message PCMCIA: Starting services (démarrage des services) ou que d'autres choses surprenantes se produisent, vous pouvez empêcher le démarrage de PCMCIA lors du prochain amorçage en saisissant `NOPCMCIA=yes` à l'invite d'amorçage. Pour limiter encore plus le risque d'erreur, chargez ensuite les trois modules de base du système PCMCIA utilisé, l'un après l'autre, manuellement.

Pour charger un module PCMCIA manuellement, utilisez, les commandes `modprobe pcmcia_core`, `modprobe yenta_socket` et `modprobe ds`

en tant qu'utilisateur root. Dans quelques rares cas, l'un des modules tcic, i82365 ou i82092 doit être utilisé à la place de yenta_scoket. Les modules critiques sont les deux premiers chargés.

Si l'erreur survient lors du chargement de pcmcia_core, reportez-vous à la page de manuel de pcmcia_core(4). Les options qu'elle décrit peuvent tout d'abord être testées avec la commande modprobe. Nous pouvons, à titre d'exemple, utiliser la vérification de domaines d'E/S (I/O) libres. Cette vérification isolée peut poser un problème si d'autres composants matériels s'en trouvent perturbés. On peut éviter ce problème à l'aide de l'option probe_io=0 :

```
modprobe  pcmcia_core probe_io=0
```

Si l'option sélectionnée donne satisfaction, attribuez la valeur probe_io=0 à la variable PCMCIA_CORE_OPTS dans le fichier /etc/sysconfig/pcmcia. Si vous souhaitez utiliser plusieurs options, séparez-les par des espaces :

```
PCMCIA_CORE_OPTS="probe_io=0 setup_delay=10"
```

Une erreur lors du chargement du module yenta_socket signifie un problème fondamental, tel que, par exemple, la répartition des ressources par ACPI.

Les fichiers /etc/pcmcia/config et /etc/pcmcia/config.opts sont exploités par le gestionnaire de cartes. Les réglages qu'ils contiennent sont utiles en partie lors du démarrage de cardmgr et en partie lors du chargement des modules pilotes pour les cartes PC. Vous pouvez aussi inclure ou exclure des IRQ, des ports d'E/S et des domaines mémoire dans le fichier /etc/pcmcia/config.opts. Dans quelques cas rares, l'accès à un mauvais domaine d'E/S peut planter tout le système. Dans ce cas, limiter en partie le domaine peut résoudre le problème.

14.5.2 La carte PCMCIA ne fonctionne pas correctement

Il existe à ce sujet essentiellement trois variantes d'erreur : la carte n'est pas reconnue, le pilote ne peut pas être chargé ou le port préparé par le pilote a été mal configuré. Vous devez vérifier si la carte est traitée par le gestionnaire de cartes ou par hotplug. Le gestionnaire de cartes gère les cartes PC Card et hotplug les cartes CardBUS.

Pas de réaction lorsqu'une carte est insérée
Lorsque le système ne réagit pas à l'insertion d'une carte et que même la saisie manuelle de `cardctl insert` ne provoque aucune réaction, l'attribution des interruptions aux périphériques PCI n'est peut-être pas correcte. Souvent, d'autres périphériques PCI que la carte réseau ont des problèmes. Dans ce cas, le paramètre d'amorçage `pci=noacpi` ou d'autres paramètres PCI ou ACPI peuvent être utile.

La carte n'est pas détectée Si la carte n'est pas détectée, le message unsupported Card in Slot x apparaît dans le fichier `/var/log/messages`. Ce message indique seulement que le gestionnaire de cartes ne peut associer aucun pilote à la carte. Les fichiers `/etc/pcmcia/config` ou `/etc/pcmcia/*.conf` sont nécessaires pour réaliser cette attribution. Ces fichiers sont, pour ainsi dire, la base de données des pilotes. Cette base de données de pilotes peut facilement être complétée en prenant ses entrées existantes comme modèle. Vous pouvez utiliser la commande `cardctl ident` pour découvrir la manière dont la carte s'identifie. Vous trouverez plus d'informations à ce sujet dans le HOWTO PCMCIA (section 6) et dans la page de manuel de pcmcia(5). Une fois le fichier `/etc/pcmcia/config` ou `/etc/pcmcia/*.conf` modifié, l'attribution des pilotes doit à nouveau être chargée ; cela se fait à l'aide de la commande `rcpcmcia reload` .

Le pilote n'est pas chargé L'une des raisons de ce type de problème est qu'une mauvaise attribution est enregistrée dans la base de données des pilotes. Cela peut, par exemple, être dû au fait qu'un fabricant a intégré une autre puce dans un modèle de carte apparemment non modifié. Parfois, il existe aussi d'autres pilotes qui fonctionnent mieux sur certains modèles que le pilote réglé par défaut (ou qui sont même les seuls à fonctionner d'ailleurs). Dans ces cas, vous avez besoin d'informations précises au sujet de la carte. Vous pouvez aussi obtenir de l'aide sur une liste de discussion ou en contactant le service d'assistance avancé (en anglais, Advanced Support Service).

Pour les cartes Cardbus, il faut saisir l'entrée `HOTPLUG_DEBUG=yes` dans le fichier `/etc/sysconfig/hotplug`. On obtient alors des messages dans le journal du système qui indique si le pilote a été chargé (avec succès).

Une autre raison peut être un conflit de ressources. Pour la plupart des cartes PCMCIA, l'IRQ, le port d'E/S ou le domaine mémoire avec lesquels elles sont exploitées n'ont aucune importance, mais il peut y avoir des exceptions.

Il convient donc de ne tester qu'une seule carte à la fois et d'interrompre momentanément les autres composants système tels que, par exemple, les cartes son, l'IrDA, le modem ou l'imprimante.

Vous pouvez, en tant qu'utilisateur root, consulter la répartition des ressources du système à l'aide de la commande lsdev. Il est absolument normal que plusieurs appareils PCI utilisent le même IRQ.

Une solution possible consiste à trouver une option appropriée pour le module du pilote de la carte à l'aide de modinfo ⟨*pilote*⟩.

La plupart des modules ont une page de manuel qui leur est consacrée. rpm -ql pcmcia | grep man énumère toutes les pages de manuel du paquetage pcmcia. Pour tester les options, les pilotes des cartes peuvent aussi être déchargés à la main.

Lorsque vous avez trouvé une solution,

vous pouvez autoriser ou interdire l'utilisation d'une ressource particulière de manière universelle dans le fichier /etc/pcmcia/config.opts. Les options pour les pilotes de cartes peuvent également être entrées dans ce fichier. Si, par exemple, le module pcnet_cs doit exclusivement être exploité avec l'IRQ 5, saisissez l'entrée suivante :

```
module pcnet_cs opts irq_list=5
```

L'interface est mal configurée Dans ce cas, nous vous conseillons de vérifier à nouveau la configuration de l'interface et le nom de la configuration à l'aide de getcfg pour exclure toute erreur de configuration éventuelle. À cette fin, attribuez la valeur yes aux variables DEBUG et HOTPLUG_DEBUG dans les fichiers respectifs /etc/sysconfig/network/config et /etc/sysconfig/hotplug. Pour les autres cartes ou si cette modification n'est d'aucun secours, vous pouvez encore ajouter la ligne set -vx dans le script exécuté par le gestionnaire de cartes ou par hotplug (reportez-vous à /var/log/messages). Cela permet d'ordonner que chaque commande du script soit systématiquement enregistrée dans le journal du système. Si vous avez détecté le point critique dans un script, vous pouvez aussi saisir les commandes correspondantes dans un terminal et les y tester.

14.6 Informations complémentaires

Vous trouverez des informations pratiques relatives à des particuliers d'ordinateurs portables sur le site web Linux Laptop http://linux-laptop.net. Une autre source d'informations intéressante est le site web de TuxMobil http://tuxmobil.org/. Vous y trouverez des howto pour les portables et l'IrDA ainsi que bien d'autres informations. En outre, vous trouverez aussi dans la base de données support plusieurs articles sur l'utilisation de Linux sur les appareils portables. Entrez les mots-clés *notebook* ou *laptop* dans le masque de recherche.

System Configuration Profile Management

Ce chapitre vous présente SCPM (en anglais, System Configuration Profile Management). SCPM vous aide à adapter la configuration de votre ordinateur à des modifications de l'environnement de travail ou de la configuration du matériel. SCPM gère un jeu de profils de système qui sont configurés en fonction des différents scénarios. Une simple commutation d'un profil de système à un autre dans SCPM remplace la reconfiguration manuelle du système.

Il existe des situations exigeant que la configuration du système soit modifiée. On rencontre souvent cette situation lorsqu'un ordinateur portable est utilisé sur différents sites. Il est également possible, toutefois, que l'on doive utiliser temporairement d'autres composants matériels sur un ordinateur de bureau. Il peut arriver également que l'on souhaite simplement expérimenter quelque chose. Dans tous les cas, il importe que la restauration du système initial soit simple à réaliser, l'idéal étant que ce changement de configuration soit aisément reproductible. SCPM permet de définir une partie de la configuration système dont on peut disposer librement, et dont les différents états peuvent être enregistrés dans des profils de configuration séparés.

La configuration réseau d'ordinateurs portables constitue probablement le principal domaine d'utilisation de SCPM. Toutefois, des configurations réseau différentes ont généralement des incidences sur d'autres éléments tels que la configuration de la messagerie ou celle des serveurs de proximité. À cela s'ajoutent aussi les différentes imprimantes utilisées au bureau et à la maison, une configuration personnalisée du serveur X pour les projecteurs servant lors de présentations, ou encore des paramètres d'économie d'énergie pour l'alimentation du portable en déplacement, ou les différents fuseaux horaires appliqués dans les implantations à l'étranger.

15.1 Terminologie

Examinons tout d'abord les principaux termes employés dans la documentation SCPM et dans le module de YaST.

- La *configuration système* fait référence à la configuration de l'ordinateur dans son ensemble. Elle recouvre tous les paramètres de base tels que, par exemple, les partitions des disques durs ou la configuration réseau, la définition des fuseaux horaires ou la configuration du clavier.
- Un *profil* ou un *profil de configuration* est un état de la configuration système qui a été enregistré et peut être restauré si nécessaire.
- Le *profil actif* est toujours le dernier profil activé. Cela ne signifie pas que la configuration système courante correspond exactement à ce profil, dans la mesure où la configuration est modifiable à tout moment.
- Les *ressources* dans la terminologie SCPM correspondent à tous les éléments contribuant à la configuration du système. Cela peut être un fichier ou un lien symbolique avec ses méta-données telles que l'utilisateur, les privilèges ou l'heure et la date d'accès. Il peut également s'agir d'un service système s'exécutant dans un profil et désactivé dans un autre.

- Les ressources sont organisées au sein de *groupes de ressources*. Ces groupes comportent des ressources formant un tout logique. Cela signifie, pour la plupart des groupes, qu'ils comportent un service et les fichiers de configuration correspondants. Ce mécanisme offre un moyen simple pour combiner des ressources manipulées par le programme SCPM, sans qu'il soit nécessaire de savoir quels fichiers de configuration sont requis pour chaque service. Le programme SCPM intègre une liste prédéfinie de groupes de ressources activés, qui devrait normalement être suffisante pour la plupart des utilisateurs.

15.2 Configuration de SCPM à la ligne de commande

Cette section introduit la configuration en ligne de commande de SCPM. Vous apprendrez ici comment démarrer SCPM, le configurer et comment travailler avec des profils.

15.2.1 Démarrage de SCPM et définition des groupes de ressources

Avant de pouvoir utiliser SCPM, il est nécessaire de l'activer au préalable. La commande`scpm enable` active SCPM. Lorsque SCPM est activé pour la première fois, il est initialisé, opération qui dure quelques secondes. SCPM peut être désactivé à tout moment à l'aide de la commande `scpm disable` afin d'éviter des changements de profils non souhaités. Après avoir été réactivé, SCPM se remet simplement à fonctionner.

SCPM gère par défaut les paramètres de réseau et d'impression ainsi que la configuration de X.Org. Dans le cas où vous souhaiteriez gérer d'autres services ou fichiers de configuration, vous devez activer les groupes de ressource correspondants. Vous pouvez lancer la commande `scpm list_groups` pour afficher les groupes de ressources déjà définis. La commande `scpm list_groups -a` permet d'afficher uniquement les groupes activés. Les commandes en ligne de commande doivent être exécutées en tant qu'administrateur `root`.

```
scpm list_groups -a

nis                     Network Information Service client
mail                   Mail subsystem
ntpd                  Network Time Protocol daemon
xf86                   X Server settings
autofs                Automounter service
network             Basic network settings
printer               Printer settings
```

Vous pouvez activer et désactiver les groupes avec `scpm activate_group NAME` ou `scpm deactivate_group NAME`, en remplaçant `NAME` par le nom de groupe correspondant.

15.2.2 Création et gestion de profils

Dès que SCPM a été activé, il existe un profil `default`. La commande `scpm list` affiche la liste de tous les profils disponibles. Ce profil existant est également le profil actif. Le nom du profil actif est affiché à l'aide de la commande `scpm active`. Le profil `default` est conçu comme la configuration par défaut servant de base pour décliner les autres profils. Il est donc recommandé de commencer par définir les paramètres communs à l'ensemble des profils. La commande `scpm reload` permet ensuite d'enregistrer ces modifications dans le profil actif. Toutefois, le profil `default` peut être copié et renommé sans restriction comme base pour de nouveaux profils.

L'ajout d'un nouveau profil peut se faire de deux façons. Si l'on veut que le nouveau profil (intitulé ici `work`) soit par exemple basé sur le profil `default`, il convient de lancer la commande `scpm copy default work`. On peut ensuite passer au nouveau profil à l'aide de la commande `scpm switch work` puis le configurer. Il peut arriver que vous modifiez la configuration système pour répondre à des besoins particuliers et que vous souhaitiez la conserver par la suite dans un nouveau profil. Il convient alors d'exécuter la commande `scpm add work`. La configuration système est alors enregistrée dans le profil`work` qui apparaît comme étant le profil actif ; cela signifie que la commande `scpm reload` enregistre les modifications dans le profil `work`.

Il est bien entendu possible de renommer ou de supprimer des profils. Ces opérations sont réalisées respectivement par les commandes `scpm rename x y` et `scpm delete z`. Ainsi, si l'on veut, par exemple, remplacer le nom `work` par `travail`, il faut lancer la commande `scpm`

`rename work travail`. Si `travail` doit ensuite être effacé, utilisez la commande `scpm delete travail`. Le profil actif, quant à lui, ne peut pas être supprimé.

15.2.3 Commuter entre profils de configuration

Pour commuter d'un profil à un autre (ici `work`), on utilise la commande `scpm switch work`. Il est permis de commuter vers le profil actif pour enregistrer dans ce profil les modifications qui ont été apportées à la configuration système. Ceci correspond à la commande `scpm reload`.

Dans un premier temps, SCPM vérifie quelles ressources du profil actif ont été modifiées depuis le dernier commutation. Pour chacune de ces ressources, SCPM demande ensuite si ces modifications doivent être copiées dans le profil actif ou abandonnées. Si (comme dans les version antérieures de SCPM) vous préférez afficher les différentes ressources séparément, exécutez la commande switch avec le paramètre `-r`, par exemple : `scpm switch -r work`.

```
scpm switch -r work

Checking for modified resources
Checking for Resources to be started/shut down
Checking for dependencies
Restoring profile default
```

SCPM compare ensuite la configuration système actuelle avec le nouveau profil vers lequel commuter. Cela permet à SCPM d'identifier les services système qui doivent être arrêtés ou (re)démarrés en fonction des changements de configuration ou de dépendances croisées. Cette opération s'apparente à un redémarrage du système, à ceci près que celui-ci ne concerne qu'une partie du système et que le reste continue à fonctionner sans modification. Les services système sont alors arrêtés, toutes les ressources modifiées, telles que les fichiers de configuration, sont enregistrées et les services système sont redémarrés.

15.2.4 Paramètres de profil avancés

Vous pouvez saisir, pour chaque profil, une description qui sera ensuite affichée à l'aide de la commande `scpm list`. Cette description peut être saisie pour le profil actif à l'aide de la commande `scpm set description "text"`. Il est par ailleurs nécessaire de spécifier les profils qui ne sont pas actifs, par exemple,

`scpm set description "text" work`. Il arrive parfois qu'en basculant sur un autre profil, il soit nécessaire d'exécuter des actions supplémentaires qui n'ont pas encore été prévues dans SCPM. La solution consiste à lier à chaque profil jusqu'à quatre programmes ou scripts exécutables qui seront exécutés à différents repères temporels du commutation. Ces repères sont les suivants :

prestop avant l'arrêt de services au moment de quitter le profil

poststop après l'arrêt de services au moment de quitter le profil

prestart avant le démarrage de services au moment d'activer le profil

poststart après le démarrage de services au moment d'activer le profil

Ajoutez ces actions avec la commande `set` en saisissant `scpm set prestop nomfichier`, `scpm set poststop nomfichier`, `scpm set prestart nomfichier` ou `scpm set poststart nomfichier`. Le fichier en question doit être un programme exécutable et spécifier l'interpréteur à utiliser.

Avertissement

Intégration de scripts personnalisés

Les scripts exécutables par SCPM doivent également être lisibles et exécutables par le superutilisateur (`root`). L'accès à ces fichiers devraient être interdits à tous les autres utilisateurs. Utilisez les commandes `chmod 700 nomfichier` et `chown root:root nomfichier` pour attribuer uniquement à `root` les droits sur ces fichiers.

Avertissement

Tous les paramètres supplémentaires saisis à l'aide de la commande `set` peuvent être consultés à l'aide de la commande `get`. La commande `scpm get poststart`, par exemple, fournit le nom du programme poststart ou bien ne fournit tout simplement aucune information, lorsque rien n'a été associé au programme poststart. De tels paramètres sont supprimés en les écrasant avec `""`. Ainsi, la commande `scpm set prestop ""` supprime le programme prestop.

De manière analogue à la création de la description, toutes les commandes `set` et `get` peuvent être appliquées à n'importe quel profil. Il convient alors de préciser le nom du profil en question. Ainsi, on a les commandes `scpm set prestop nomfichier work` et `scpm get prestop work`.

15.3 Le gestionnaire de profils de YaST

Démarrez le gestionnaire de profils de YaST dans le centre de contrôle YaST ('Système' → 'Gestionnaire de profils'). Lors du premier démarrage, activez SCPM de façon explicite en sélectionnant 'Activer' dans le dialogue 'Options SCPM', comme dans la figure 15.1 de la présente page. Dans 'Paramètres', définissez si les fenêtres contextuelles doivent se refermer automatiquement et s'il faut afficher des messages relatifs à la progression de votre configuration SCPM. Pour 'Mode de commutation', déterminez si les ressources modifiées du profil actif doivent être enregistrées ou abandonnées lorsque le profil est commuté. Si le 'Mode de commutation' est défini comme 'Normal', toutes les modifications dans le profil actif sont enregistrées lors de la commutation. Pour définir le comportement de SCPM lors de l'amorçage, spécifiez 'Enregistrer les modifications' (paramètre par défaut) ou 'Abandonner les modifications' pour le 'Mode d'amorçage'.

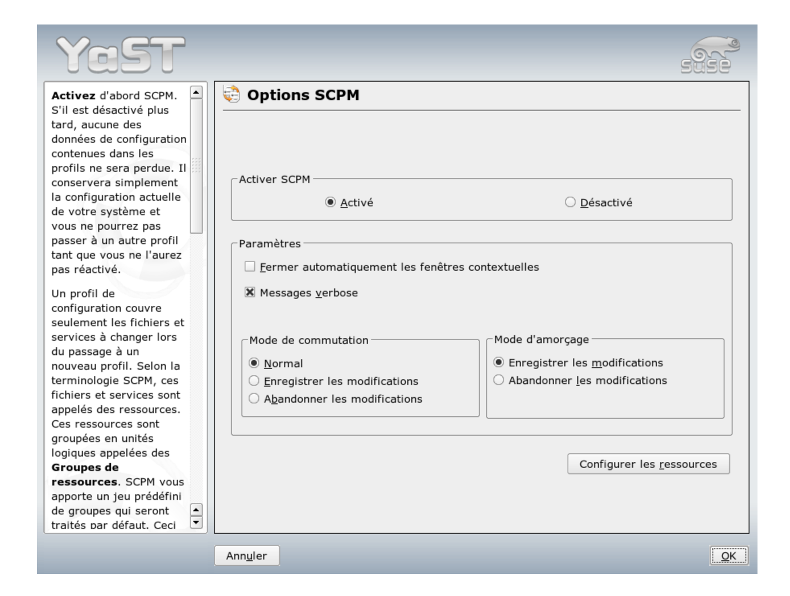


FIG. 15.1: *Options SCPM de YaST*

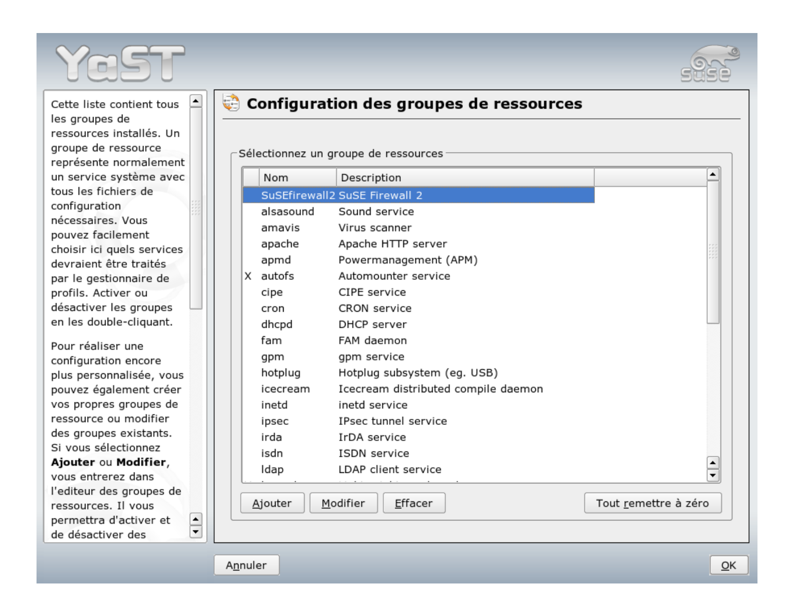


FIG. *15.2: Configuration des groupes de ressources*

15.3.1 Configuration des groupes de ressources

Pour modifier la configuration actuelle de ressources, sélectionnez 'Configurer les ressources' dans le dialogue 'Options SCPM'. Le dialogue suivant, 'Configuration des groupes de ressources' (voir la figure 15.2 de la présente page), affiche tous les groupes de ressources disponibles sur votre système. Pour ajouter ou modifier un groupe de ressources, spécifiez ou modifiez 'Groupe de ressources' et 'Description'. Pour un service LDAP, par exemple, saisissez `ldap` en tant que 'Groupe de ressources' et `Service client LDAP` en tant que 'Description'. Entrez alors les ressources adéquates (services, fichiers de configuration ou les deux) ou modifiez cellez qui existent déjà. Effacez celles qui ne sont pas utilisées. Pour remettre l'état des ressources sélectionnées à zéro—abandonner tous les changements effectués et retournez aux valeurs de la configuration initiale—sélectionnez 'Rétablir le groupe'. Vos changements sont enregistrés dans le profil actif.

15.3.2 Création d'un nouveau profil

Pour créer un nouveau profil, cliquez sur 'Ajouter' dans le dialogue de démarrage ('Gestion des profils de la configuration système'). Dans la fenêtre ouverte, choisissez si les nouveaux profils doivent être basés sur la configuration actuelle du système (SCPM retrouve automatiquement la configuration actuelle et l'enregistre dans votre profil) ou sur un profil existant. Si vous utilisez a configuration actuelle du système comme base du nouveau profil, vous pouvez marquer le nouveau profil comme étant le nouveau profil actif. Ceci ne change en rien l'ancien profil et ne démarre ou n'arrête aucun service.

Attribuez un nom et une courte description au nouveau profil dans le dialogue suivant. Pour que SCPM exécute des scripts spéciaux sur une commutation des profils, entrez les chemins pour chaque exécutable (voir la figure 15.3 de la présente page). Consultez la section 15.2.4 page 313 pour plus d'informations. SCPM exécute une vérification des ressources du nouveau profil. Une fois que ce test a été réussi, le nouveau profil est prêt à être utilisé.

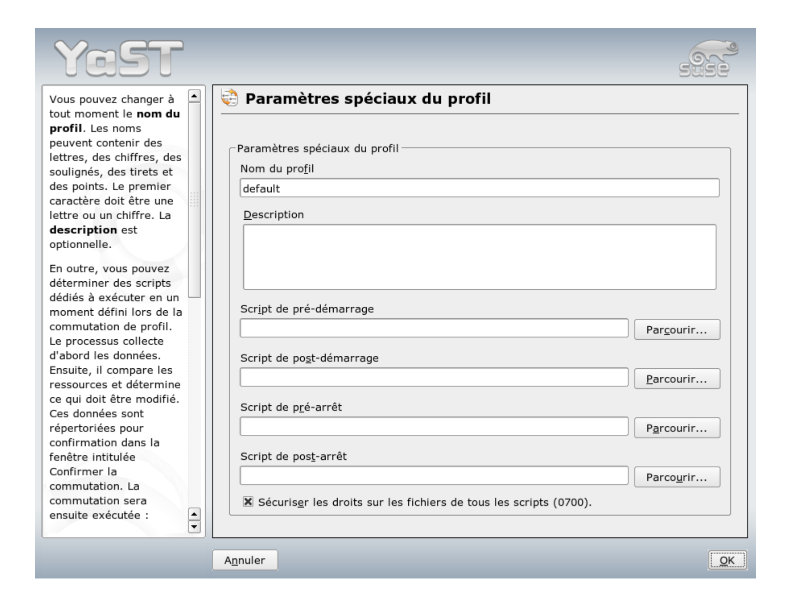


FIG. 15.3: *Paramètres spéciaux du profil*

15.3.3 Modification de profils existants

Pour modifier un profil existant, sélectionnez 'Modifier' dans le dialogue de démarrage ('Gestion des profils de la configuration système') puis modifiez le nom, la description, les scripts et les ressources selon vos besoins.

15.3.4 Commutation de profils

Pour commuter des profils, ouvrez le gestionnaire de profils. Le profil actif est marqué d'une flèche. Sélectionnez le profil vers lequel commuter et cliquez sur 'Basculer vers'. SCPM vérifie s'il y a de nouvellles ressources ou des ressources modifiées et, le cas échéant, les ajoute.

Si une ressource a été modifiée, YaST ouvre le dialogue 'Confirmer la commutation'. 'Ressources modifiées du profil actif' affiche tous les groupes de ressources du profil actif qui ont été modifiés mais pas encore enregistrés dans le profil actif. 'Enregistrer ou Ignorer' spécifie si les changements du groupe de ressources sélectionné doivent être enregistrés dans le profil actif ou s'ils doivent être abandonnés. Vous pouvez également sélectionner chaque ressource et cliquez sur 'Détails' pour analyser en détail les modifications. Ceci affiche une liste de tous les fichiers de configuration ou exécutables qui appartiennent au groupe de ressources qui a été modifié. Pour obtenir une comparaison ligne par ligne entre l'ancienne et la nouvelle version, cliquez sur 'Afficher les modifications'. Après avoir analysé les changements, décidez ce que vous voulez faire dans 'Action' :

Enregistrer la ressource Enregistre cette ressource dans le profil actif mais ne touche pas aux autres profils.

Ignorer la ressource Ne touche pas la ressource active. Le changement est abandonné.

Enregistrer dans tous les profils Copie la configuration complète de cette ressource dans tous les autres profils.

Corriger tous les profils Applique uniquement les modifications les plus récentes à tous les profils.

'Enregistrer ou Ignorer tout' enregistre ou abandonne les modifications de toutes les ressources affichées dans ce dialogue.

Une fois que vous avez confirmé les changements dans le profil actif, quittez le dialogue 'Confirmer la commutation' en cliquant sur 'OK'. SCPM bascule alors vers le nouveau profil. Lors de la commutation, il exécute les scripts prestop et poststop de l'ancien profil et les scripts prestop et poststop du nouveau profil.

15.4 Problèmes possibles et solutions

Cette section traite des problèmes fréquemment rencontrés avec SCPM. Vous apprendrez ici dans quel cas ces problèmes arrivent et comment les résoudre.

15.4.1 Interruption lors d'une opération de commutation

Il peut arriver, dans certaines conditions, qu'une erreur d'exécution interrompe SCPM lors d'une opération de commutation. Cet événement peut être dû à des facteurs extérieurs tels que, par exemple, une interruption par l'utilisateur, la batterie de l'ordinateur portable qui est déchargée ou même une erreur du programme SCPM lui-même. Dans ce cas, vous obtiendrez à la prochaine exécution de SCPM un message indiquant que SCPM est verrouillé. Cette mesure vise à protéger votre système, dans la mesure où les données enregistrées par SCPM dans sa base de données sont probablement incompatibles avec l'état de votre système. Pour résoudre ce problème, exécutez `scpm recover`. SCPM réalise alors toutes les opérations de l'exécution précédente. Vous pouvez également exécuter la commande `scpm recover -b` qui essaie d'annuler toutes les opérations déjà réalisées lors de l'exécution précédente. Si vous utilisez le gestionnaire de profils de YaST, vous obtiendrez un dialogue de récupération au démarrage qui vous offre la possibilité d'exécuter les commandes décrites ci-dessus.

15.4.2 Modification de la configuration du groupe de ressources

Si vous souhaitez modifier la configuration du groupe de ressources alors que SCPM a déjà été initialisé, exécutez la commande `scpm rebuild` après avoir ajouté ou supprimé des groupes. Cette opération ajoute de nouvelles ressources à tous les profils et supprime définitivement celles qui ont été retirées. Si vous avez configuré les ressources effacées différemment dans les divers profils, ces données de configuration sont alors perdues sauf, bien entendu, pour la version actuelle de votre système qui n'est pas touchée par SCPM. Dans le cas où vous décidez de modifier la configuration avec YaST il n'est pas nécessaire de faire de reconstruction (rebuild), cette opération étant assurée par YaST à votre place.

15.5 Choix du profil lors de l'amorçage du système

Si vous souhaitez choisir un profil dès l'amorçage du système, il suffit de presser F4 lorsque l'écran de démarrage apparaît pour afficher les profils disponibles et sélectionner le profil souhaité avec les touches de direction. Confirmez votre choix avec Enter et le profil sélectionné sera proposé comme option d'amorçage.

15.6 Informations complémentaires

Vous trouverez la documentation la plus récente dans les pages d'information de SCPM. Vous pouvez les visualiser avec des outils tels que Konqueror ou Emacs (`konqueror info:scpm`). Dans un terminal, utilisez `info` ou `pinfo`. Des informations pour les développeurs se trouvent sous `/usr/share/doc/packages/scpm`.

Gestion de l'énergie

Ce chapitre présente les différentes techniques de gestion de l'énergie sous Linux. La configuration de toutes les techniques possibles depuis APM (en anglais, Advanced Power Management) en passant par ACPI (en anglais, Advanced Configuration and Power Interface) jusqu'à l'adaptation de la fréquence du processeur (en anglais, CPU Frequency Scaling) est détaillée ici.

De la seule gestion de l'énergie sur les portables avec APM, le développement s'est poursuivi pour parvenir à ACPI, un outil d'information et de configuration du matériel disponible sur tous les ordinateurs modernes (portables, de bureau et serveurs). Il est en outre possible d'adapter la fréquence du processeur, en fonction de chaque situation, sur de nombreux types de matériel modernes, ce qui permet, sur les appareils mobiles, d'économiser la durée de vie de la batterie (*adaptation de la fréquence du processeur* ; en anglais, CPU Frequency Scaling).

Toutes les techniques de gestion de l'énergie présupposent de disposer de matériel et de routines BIOS adaptés. La plupart des portables et de nombreux ordinateurs de bureau et serveurs modernes satisfont à cette exigence. On a souvent utilisé APM (en anglais, Advanced Power Management) sur le matériel ancien. Comme APM se compose essentiellement d'un ensemble de fonctionnalités implémenté dans le BIOS, la prise en charge APM est, selon le matériel et les circonstances, plus ou moins bonne. ACPI est bien plus complexe et varie encore plus qu'APM, pour ce qui concerne sa prise en charge, en fonction du type de matériel. C'est pour cette raison qu'il n'y aurait aucun sens à privilégier un système plutôt qu'un autre. Testez les différents procédés sur votre matériel et utilisez la technologie la mieux prise en charge.

Important

Gestion de l'énergie sur les processeurs AMD64

Les processeurs AMD64 avec un noyau 64 bits ne permettent d'utiliser qu'ACPI.

Important

16.1 Fonctionnalités d'économie d'énergie

Les fonctionnalités d'économie d'énergie ne représentent pas seulement un intérêt pour les ordinateurs portables mais également dans le cadre d'une utilisation fixe. Les fonctionnalités les plus importantes sont décrites ci-après ainsi que leur utilisation dans le cadre des deux systèmes d'économie d'énergie APM et ACPI :

Mise en attente (standby) Dans ce type de fonctionnement, seul l'écran est éteint et, pour certains appareils, les performances du processeur limitées. Certains APM ne proposent pas cette fonctionnalité. Avec ACPI, elle correspond à l'état S1 ou S2.

Mise en veille (sur mémoire) (suspend (to memory))
Dans ce mode, la totalité de l'état du système est inscrite dans la mémoire de travail et l'ensemble du système, en dehors de la mémoire de travail est mis en veille. Dans cet état, l'ordinateur n'a besoin que de très peu d'énergie. L'avantage de cet état est qu'il est possible en l'espace de quelques secondes seulement de reprendre son travail au point où l'on s'était arrêté sans avoir à amorcer l'ordinateur et à recharger les programmes nécessaires. Dans le cas des ordinateurs qui fonctionnent avec APM, il suffit souvent de rabattre l'écran en position fermée pour déclencher ce mode de veille et simplement de l'ouvrir à nouveau pour reprendre le travail. Avec ACPI, ce mode correspond à l'état S3. La prise en charge de ce mode est encore en développement et dépend donc fortement du matériel utilisé.

Hibernation (mise en veille sur disque)
Dans ce mode de fonctionnement, l'état du système est complètement enregistré sur le disque dur et le système ensuite éteint. La reprise à partir de cet état dure entre 30 et 90 secondes et dans ce cas aussi, c'est l'état exact avant la mise en veille qui est repris tel que. Certains fabricants proposent des formes hybrides de ce mode (par exemple, RediSafe pour les Thinkpads d'IBM). Avec ACPI, l'hibernation correspond à l'état S4. Sous Linux la *mise en veille sur disque* est exécutée par des routines du noyau qui sont indépendantes de APM et ACPI.

Contrôle de l'état de la batterie ACPI et APM contrôlent tous les deux l'état de charge de la batterie et affichent des messages relatifs à l'état de charge courant. En outre, ces deux systèmes coordonnent l'exécution d'actions simples lorsqu'un état de charge critique est atteint.

Mise hors tension automatique Une fois éteint, l'ordinateur est complètement mis hors tension. Cela a un sens avant tout lorsqu'un arrêt automatique est effectué, peu avant que la batterie soit vide.

Arrêt des composants système L'arrêt du disque dur apporte la contribution la plus importante à l'économie d'énergie de tout le système. Selon la fiabilité de l'ensemble du système il peut être mis en sommeil plus ou moins longtemps. Cependant, plus la période de sommeil du disque est longue, plus le risque de perte de données augmente. Vous pouvez désactiver les autres composants via ACPI (du moins théoriquement) ou, durablement, dans la configuration du BIOS.

Contrôle de la performance du processeur
Avec le processeur, il est possible d'économiser de l'énergie de trois façons différentes : l'adaptation de la fréquence et de la tension (connue aussi sous les noms PowerNow! ou Speedstep), la diminution de la cadence

(throttling) et la mise en sommeil du processeur (états C). Selon le type d'utilisation de l'ordinateur, ces différentes façons peuvent être combinées suivant vos besoins.

16.2 APM

Le BIOS APM assure seul certaines fonctionnalités d'économie d'énergie. Vous pouvez, sur de nombreux ordinateurs portables, activer la mise en attente et la mise en veille à l'aide de combinaisons de touches ou en rabattant l'écran. Le système d'exploitation ne propose, en premier lieu, aucune fonctionnalité pour ce faire. Si vous souhaitez pouvoir utiliser ce type de fonctionnement en saisissant une commande, il est recommandé d'exécuter un certain nombre d'actions avant la mise en sommeil. Pour l'affichage de l'état de charge de la batterie, des paquetages spécifiques et un noyau approprié sont nécessaires.

La prise en charge d'APM est parfaitement intégrée dans les noyaux de SUSE LINUX. Cependant, celle-ci n'est activée que si aucun ACPI n'est implémenté dans le BIOS et qu'un BIOS APM est trouvé. Pour activer la prise en charge APM, vous devez désactiver ACPI à l'invite d'amorçage en saisissant `acpi=off`. Vous pouvez facilement vérifier si APM a été activé, avec la commande `cat /proc/apm`. Si une ligne contenant divers nombres apparaît, tout est en ordre. Vous devez alors saisir une commande `shutdown -h` pour éteindre l'ordinateur.

Comme certaines implémentations de BIOS ne respectent pas les standards, on peut rencontrer des problèmes lors de l'utilisation de APM. Vous pouvez en contourner certains avec des paramètres d'amorçage particuliers. Tous les paramètres sont fournis à l'invite d'amorçage sous la forme `apm=parameter` :

on/off Activer ou désactiver la prise en charge APM

(no-)allow-ints Autoriser les interruptions pendant l'exécution des fonctions du BIOS.

(no-)broken-psr Le BIOS a une fonctionnalité "GetPowerStatus" qui ne fonctionne pas correctement.

(no-)realmode-power-off Repasser le processeur en mode réel avant l'arrêt.

(no-)debug Enregistrer les événements APM dans le journal système.

(no-)power-off Mettre le système hors tension après l'arrêt.

bounce-interval=⟨*n*⟩ Temps en centièmes de secondes au bout duquel, après un événement de mise en sommeil, les autres événements de mise en sommeil sont ignorés.

idle-threshold=⟨*n*⟩ Pourcentage d'inactivité système à partir duquel la fonctionnalité BIOS `idle` est exécutée (0=toujours, 100=jamais).

idle-period=⟨*n*⟩ Temps en centièmes de secondes au bout duquel l'(in)activité du système est mesurée.

Le démon APM apmd utilisé auparavant n'est plus utilisé. Sa fonctionnalité est contenue dans le nouveau powersaved, qui maîtrise également ACPI et la régulation de la fréquence du processeur.

16.3 ACPI

ACPI (en anglais, Advanced Configuration and Power Interface) doit permettre au système d'exploitation d'organiser et de gérer les différents composants matériel individuellement. Ainsi ACPI remplace aussi bien le Plug and Play qu'APM. ACPI fournit aussi d'autres informations diverses sur la batterie, l'alimentation en énergie, la température et le ventilateur et renseigne sur les événements système, tels que par exemple "rabattre l'écran" ou "charge de la batterie faible".

Le BIOS contient des tables dans lesquelles sont répertoriées des informations sur les différents composants et les méthodes d'accès au matériel. Ces informations sont par exemple utilisées par le système d'exploitation pour attribuer des interruptions ou mettre sous ou hors tension des composants, le cas échéant. Mais comme le système d'exploitation exécute des instructions qui se trouvent dans le BIOS, tout dépend là encore de l'implémentation du BIOS. Vous trouverez dans `/var/log/boot.msg` les messages d'amorçage. ACPI les utilise pour signaler les tables trouvées et qu'il a pu lire. Vous trouverez plus d'informations sur le dépannage des problèmes ACPI dans la section 16.3.4 page 330.

16.3.1 ACPI en pratique

Lorsque le noyau reconnaît un BIOS ACPI lors de l'amorçage, ACPI est automatiquement activé et APM désactivé. Le paramètre d'amorçage `acpi=on` peut tout au plus être utile sur les vieilles machines. L'ordinateur doit prendre en charge ACPI 2.0 ou une version plus récente. Vous pouvez vérifier si ACPI a été activé dans les messages d'amorçage du noyau, dans `/var/log/boot.msg`.

Ensuite, un certain nombre de modules doit encore être chargé. Ceux-ci sont chargés par le script de démarrage du démon ACPI. Si l'un de ces modules rencontre un problème, vous pouvez l'exclure du chargement ou du déchargement dans

/etc/sysconfig/powersave/common. Vous trouverez dans le journal du système (/var/log/messages) les messages du module et les composants qui ont été reconnus.

Vous pouvez trouver maintenant dans /proc/acpi un ensemble de fichiers qui vous informent au sujet de l'état du système ou que vous pouvez utiliser pour modifier de manière active certains états. Les fonctionnalités ne sont pas encore toutes totalement prises en charge dans la mesure où quelques unes sont encore en phase de développement et que la prise en charge de certaines dépend fortement de l'implémentation du fabricant.

Vous pouvez afficher tous les fichiers (à l'exception de dsdt et fadt) avec la commande cat. Pour certains d'entre eux, vous pouvez modifier quelques réglages en utilisant echo, par exemple, en indiquant avec echo X > fichier les valeurs appropriées pour X. Pour accéder à ces informations et possibilités de contrôle, utilisez toujours la commande powersave. Pour plus de détails, vous trouverez ci-après une description des fichiers les plus importants :

/proc/acpi/info Informations générales à propos d'ACPI

/proc/acpi/alarm Définissez ici quand le système doit reprendre après une période de sommeil. Cette fonctionnalité n'est actuellement pas encore totalement prise en charge.

/proc/acpi/sleep Donne des informations sur les différents états de sommeil.

/proc/acpi/event Tous les événements sont consignés ici. Ils sont traités par le démon Powersave (powersaved). Si aucun démon n'est en train d'y accéder, vous pouvez lire les événements avec cat /proc/acpi/event (pressez Ctrl-C pour terminer). Un effleurement sur l'interrupteur de mise sous tension ou l'écran rabattu sont de tels événements.

/proc/acpi/dsdt et /proc/acpi/fadt
C'est ici que se trouvent les tables ACPI, DSDT (*Differentiated System Description Table*) et FADT (*Fixed ACPI Description Table*). Vous pouvez les lire avec les commandes acpidmp, acpidisasm et dmdecode. Vous trouverez ces programmes et la documentation correspondante dans le paquetage pmtools. Exemple : acpidmp DSDT | acpidisasm

/proc/acpi/ac_adapter/AC/state
Indique si l'ordinateur est raccordé à l'alimentation en énergie.

/proc/acpi/battery/BAT*/{alarm,info,state}
Informations détaillées sur l'état des batteries. Pour pouvoir consulter l'état de charge, vous devez comparer last full capacity dans info avec

`remaining capacity` dans `state`. Vous pouvez effectuer la même opération plus confortablement avec des programmes spéciaux tels que présentés dans la section 16.3.3 page 330. Vous pouvez préciser dans `alarm` la capacité à partir de laquelle un événement de batterie doit être déclenché.

`/proc/acpi/button` Ce répertoire contient des informations sur les différents interrupteurs.

`/proc/acpi/fan/FAN/state` Indique si le ventilateur fonctionne correctement. Vous pouvez également le mettre sous ou hors tension en inscrivant `0` (activé) ou `3` (désactivé) dans ce fichier. Attention, car aussi bien le code ACPI dans le noyau que le matériel (ou le BIOS) écrasent ce réglage en cas de trop forte chauffe.

`/proc/acpi/processor/CPU*/info`
Informations concernant les possibilités d'économie d'énergie du processeur.

`/proc/acpi/processor/CPU*/power`
Informations relatives à l'état actuel du processeur. Un astérisque à côté de `C2` signifie que le processeur est à vide ; c'est l'état le plus courant comme le laisse voir la valeur pour `usage`.

`/proc/acpi/processor/CPU*/throttling`
Vous pouvez ici configurer la réduction de la fréquence du processeur. Dans la plupart des cas, il est possible de procéder à huit niveaux de réduction. Ceci est indépendant de l'adaptation de la fréquence.

`/proc/acpi/processor/CPU*/limit`
Lorsque la performance (désuet) et l'étranglement (en anglais throttling) sont automatiquement réglés par un démon, indiquez ici les limites à ne pas dépasser. Il existe des limites définies par le système et certaines qui peuvent être réglées par l'utilisateur.

`/proc/acpi/thermal_zone/` Un sous-répertoire est prévu ici pour chaque zone thermique. Une zone thermique est un domaine avec des propriétés thermiques semblables ; leur nombre et leur nom est choisi par le fabricant de matériel informatique. Les nombreuses possibilités proposées par ACPI sont cependant rarement implémentées. En revanche, la gestion de la température est effectuée de manière classique, directement par le BIOS, sans accorder le moindre droit à la parole au système d'exploitation car c'est tout simplement la durée de vie du matériel qui est ici en jeu. Les descriptions ci-après sont donc partiellement théoriques.

`/proc/acpi/thermal_zone/*/temperature`
La température actuelle de la zone thermique.

/proc/acpi/thermal_zone/*/state
L'état indique si tout est `ok` ou si ACPI assure un refroidissement `actif` ou `passif`. Pour les systèmes de ventilation indépendants d'ACPI, l'état est toujours `ok`.

/proc/acpi/thermal_zone/*/cooling_mode
Vous pouvez choisir ici la méthode de refroidissement contrôlée par ACPI ; passive (moins de performances mais économique) ou active (100 % de performance et 100 % du bruit du ventilateur).

/proc/acpi/thermal_zone/*/trip_points
Vous pouvez définir ici à partir de quelle température une mesure doit être entreprise. Les options possibles varient entre un refroidissement passif ou actif jusqu'à la mise en sommeil (`hot`) voire à la mise hors tension de l'ordinateur (`critical`). Les actions possibles sont définies, selon les appareils, dans la table DSDT. Les points de déclenchement définis dans les spécifications ACPI sont : `critical`, `hot`, `passive`, `active1` et `active2`. Même s'ils ne sont pas tous implémentés, vous devez, lorsque vous écrivez dans le fichier `trip_points`, les saisir tous dans cet ordre. Ainsi une entrée comme `echo 90:0:70:0:0 > trip_points` correspond à une température de `90` pour `critical` et de `70` pour `passive` (toutes les températures sont mesurées en degrés Celsius).

/proc/acpi/thermal_zone/*/polling_frequency
Lorsque la valeur dans `temperature` n'est pas automatiquement mise à jour, dès que la température varie, il est possible ici de passer au mode d'interrogation (en anglais, polling mode). La commande `echo X > /proc/acpi/thermal_zone/*/polling_frequency` implique que la température est sondée toutes les `X` secondes. Utilisez `X=0` pour désactiver l'interrogation.

Vous n'avez pas besoin de régler manuellement ces informations, configurations et événements. Pour cela, vous disposez du démon Powersave (powersaved) et de différentes applications telles que powersave, kpowersave et wmpowersave (voir la section 16.3.3 page 330). Étant donné que powersaved contient les fonctionnalités de l'ancien acpid, celui-ci n'est plus nécessaire.

16.3.2 Contrôle de la performance du processeur

Avec le processeur, il est possible d'économiser de l'énergie de trois façons différentes qui, selon le type d'utilisation de l'ordinateur peuvent être combinées suivant vos besoins. Économie d'énergie signifie également que le système chauffe moins et qu'il sollicite donc moins la ventilation.

Adaptation de la fréquence et de la tension
PowerNow! et Speedstep sont les noms donnés par les entreprises AMD et Intel pour cette technique qui existe aussi dans les processeurs d'autres fabricants. Ici, la fréquence du processeur et sa tension intrinsèque sont toutes deux diminuées. L'avantage réside dans une économie d'énergie plus que linéaire. C'est à dire que pour une fréquence (et donc une performance) diminuée de moitié, c'est nettement plus que la moitié de l'énergie qui est économisée. Cette technique fonctionne indépendamment de APM ou de ACPI et nécessite un démon qui régule la fréquence et les performances requises. Les paramètres peuvent être configurés dans le répertoire `/sys/devices/system/cpu/cpu*/cpufreq/`.

Réduction de la cadence d'horloge Cette technique est connue sous le nom de throttling. Ici, un certain pourcentage des cycles d'horloge du processeur est supprimé. Un quart est supprimé pour un étranglement de 25%, et pour un étranglement de 87,5%, il n'y a plus qu'un huitième des cycles d'horloge. Cependant, l'économie d'énergie n'est pas tout à fait linéaire. On utilise le throttling uniquement lorsqu'il n'y a pas de régulation de la fréquence ou pour une économie maximale. Cette technique doit également être contrôlée par un processus propre. L'interface du système est `/proc/acpi/processor/*/throttling`.

Mise en sommeil du processeur Le processeur est toujours mis en sommeil par le système d'exploitation lorsqu'il n'y a rien à faire. Dans ce cas, le système d'exploitation envoie au processeur l'instruction `halt` prévue à cet effet. Il existe différents niveaux : C1, C2 et C3. Dans l'état C3, le plus économique, même le processus de comparaison de la mémoire cache du processeur avec la mémoire principale est arrêté ; cet état ne peut donc être pris que lorsqu'aucun périphérique ne modifie le contenu de la mémoire principale par activité de bus maître. Certains pilotes empêchent ainsi l'utilisation de C3. L'état courant est affiché dans `/proc/acpi/processor/*/power`.

L'adaptation de la fréquence comme la réduction de la cadence d'horloge ne sont intéressants que lorsque le processeur a quelque chose à faire car dans le cas contraire, ce sont les états C, plus économiques qui sont favorisés. Cependant, lorsque le processeur est occupé, la régulation de la fréquence est la meilleur méthode d'économie d'énergie. Souvent, le processeur n'est que partiellement occupé. Une fréquence réduite lui suffit alors pour fonctionner. En général, l'adaptation dynamique de la fréquence à l'aide d'un démon, tel que powersaved, est la meilleure solution. Lorsque l'ordinateur fonctionne sur batterie ou lorsqu'il doit ne doit pas chauffer, c'est à dire être silencieux, la spécification d'une fréquence basse définie statiquement peut être préférable.

Le throttling ne devrait être utilisé qu'en dernière extrémité lorsque l'on souhaite, par exemple, augmenter la durée de vie des batteries malgré le fonctionnement du système. Cependant, certains systèmes ne fonctionnent plus correctement lorsque l'étranglement est trop important. La suppression de cycles d'horloge n'est d'aucun intérêt lorsque le processeur n'a que peu à faire.

Le démon powersave contrôle aussi ces technologies sous SUSE LINUX. La configuration nécessaire à cette fin est décrite dans la section 16.5 page 333.

16.3.3 Outils ACPI

Il existe un grand nombre d'outils ACPI plus ou moins volumineux, notamment des outils d'informations purs, qui indiquent l'état de la batterie, la température, etc. (acpi, klaptopdaemon, wmacpimon, etc.). D'autres facilitent l'accès aux structures sous `/proc/acpi` ou aident à observer les modifications (akpi, acpiw, gtkacpiw). De plus, il existe aussi des outils pour le traitement des tables ACPI dans le BIOS (paquetage `pmtools`).

16.3.4 Problèmes possibles et solutions

Il existe deux groupes de problèmes différents. D'une part, il peut naturellement y avoir des erreurs dans le code ACPI du noyau qui n'ont pas encore été relevées. D'autre part, il peut toutefois y avoir une solution à télécharger. Les problèmes au niveau du BIOS de l'ordinateur sont malheureusement moins agréables et aussi plus fréquents. Il arrive malheureusement que des écarts aient été insérés par rapport aux spécifications ACPI du BIOS pour contourner des erreurs de l'implémentation ACPI dans d'autres systèmes d'exploitation très développés. Il existe aussi du matériel connu pour ses erreurs graves dans l'implémentation ACPI et qui est donc répertorié dans une liste noire afin de ne pas utiliser dessus ACPI pour le noyau Linux.

En cas de problème, la première chose à faire est la mise à jour du BIOS. Si l'ordinateur n'amorce pas du tout, l'un des paramètres d'amorçage suivants peut se révéler utile :

pci=noacpi Ne pas utiliser ACPI pour la configuration des appareils PCI.

acpi=oldboot Ne procéder qu'aux configurations de ressources simples, sinon, ne pas utiliser ACPI.

acpi=off Nésactiver ACPI.

Avertissement

Problèmes lors de l'amorçage sans ACPI

Certains ordinateurs de la nouvelle génération, notamment les systèmes SMP et AMD64, ont besoin d'ACPI pour configurer correctement le matériel. Si l'on désactive ACPI, cela peut engendrer des problèmes.

Avertissement

Surveillez bien les messages du système lors de l'amorçage. Utilisez pour cela la commande `dmesg | grep -2i acpi` après l'amorçage (ou alors on affiche tous les messages, car ACPI n'est pas nécessairement responsable du problème). En cas d'erreur lors de l'analyse d'une table ACPI, vous avez la possibilité, du moins pour la table la plus importante, la table DSDT, de créer une table corrigée dans un noyau individuel. La DSDT erronée du BIOS est par la suite ignorée. La procédure à suivre est détaillé dans la section 16.5.4 page 339.

Vous disposez, lors de la configuration du noyau, d'un interrupteur pour activer les messages de débogage d'ACPI. Lors de la compilation et de l'installation d'un noyau avec débogage ACPI, cela peut fournir des informations détaillées aux experts à la recherche d'erreurs.

En cas de problèmes relatifs au BIOS ou au matériel, il est toujours judicieux de s'adresser au fabricant de l'appareil. Même quand ces derniers ne sont pas toujours d'un grand secours lorsqu'il s'agit d'un système fonctionnant sous Linux, il est important de les informer d'éventuels problèmes. Ce n'est que lorsque les fabricants auront remarqué que suffisamment de leurs clients optent pour Linux qu'ils prendront le problème au sérieux.

Informations complémentaires

Vous trouverez plus de documentation et d'aide relatives à ACPI dans :

- `http://www.cpqlinux.com/acpi-howto.html` (HowTo ACPI détaillé, contient des correctifs de la DSDT)
- `http://www.intel.com/technology/iapc/acpi/faq.htm` (FAQ ACPI chez Intel)
- `http://acpi.sourceforge.net/` (Le projet ACPI4Linux de Sourceforge)
- `http://www.poupinou.org/acpi/` (Correctifs DSDT de Bruno Ducrot)

16.4 Pause du disque dur

Le disque dur peut être complètement arrêté sous Linux lorsqu'il n'est pas utilisé ou lorsque vous utilisez un mode économique ou silencieux. Cependant, notre expérience montre qu'il n'est pas intéressant, dans le cas de ordinateurs portables modernes, d'arrêter en partie un disque dur car ceux-ci se mettent d'eux-mêmes dans un mode économique lorsqu'ils ne sont pas utilisés. Néanmoins, si vous souhaitez être particulièrement économe, vous pouvez tester l'une des possibilités suivantes. La plupart des fonctionnalités peuvent être contrôlées à l'aide de powersaved.

Le programme hdparm est utilisé pour procéder à différents réglages du disque dur. L'option `-y` permet de mettre le disque immédiatement en attente, l'option `-Y` (attention) permet de l'arrêter complètement. `hdparm -S x` permet d'arrêter le disque dur après une certaine durée d'inactivité. Le joker ⟨*x*⟩ a la signification suivante : `0` arrête ce mécanisme, le disque dur fonctionne toujours. Les valeurs de `1` à `240` sont multipliées par cinq secondes. `241` à `251` correspondent à entre 1 et 11 fois 30 minutes.

Les possibilités d'économie d'énergie internes au disque dur sont contrôlées à l'aide de l'option `-B`. Ici, il est possible de choisir un nombre entre `0` (économie maximale) et `255` (performance maximale). Le résultat dépend du disque utilisé et est difficile à juger. Pour qu'un disque dur soit plus silencieux, l'option `-M` peut être utilisée. Ici aussi, on choisit une valeur entre `128` (silencieux) et `254` (rapide).

Il n'est cependant pas toujours si facile d'écrire des données sur le disque dur, puis de redémarrer le disque, car il existe sous Linux un grand nombre de processus qui gardent toujours le disque dur éveillé. Il est donc capital que vous compreniez à présent la manière dont Linux traite les données qui doivent être écrites sur le disque dur. Toutes les données sont tout d'abord enregistrées de manière intermédiaire dans une mémoire tampon de la mémoire de travail. Ce tampon est surveillé par le démon de mise à jour du noyau (kupdated). À chaque fois que des données atteignent un certain âge ou que le tampon atteint un certain niveau de remplissage, le tampon est vidé et les données écrites sur le disque dur. La taille du tampon est du reste dynamique et dépend de la taille de la mémoire et du degré d'exploitation du système. Comme l'objectif principal est la sécurité des données, kupdated est réglé par défaut sur de petits intervalles de temps. Il vérifie la mémoire tampon toutes les 5 secondes et informe le démon bdflush lorsque les données ont plus de 30 secondes ou quand le tampon est rempli à 30 %. Le démon bdflush écrit alors les données sur le disque dur. Il les écrit aussi sans se soucier de kupdated quand, par exemple, le tampon est rempli.

Avertissement

Atteinte à la sécurité des données

Les modifications des réglages du démon de mise à jour du noyau mettent en danger la sécurité des données.

Avertissement

Outre tous ces processus, les systèmes de fichiers journalisés tels que, par exemple, ReiserFS ou Ext3 écrivent leurs méta-données sur le disque dur indépendamment de bdflush, ce qui empêche naturellement une mise en sommeil du disque dur. Pour l'éviter, il existe à présent une extension dans le noyau qui a été tout spécialement développée pour les appareils mobiles. Vous en trouverez une description précise dans le fichier `/usr/src/linux/Documentation/laptop-mode.txt`.

Il faut, en outre, surveiller la manière dont les programmes que vous utilisez déjà se comportent. Ainsi, les bons éditeurs de texte écrivent régulièrement des sauvegardes cachées des données qui viennent d'être modifiées sur le disque dur, avec pour conséquence que le disque dur est sans arrêt sollicité. Vous pouvez inhiber ce type de comportements des programmes, mais ici aussi au prix de la sécurité des données.

À ce propos, il existe pour le démon de messagerie postfix une variable `POSTFIX_LAPTOP`. Si celle-ci a la valeur `yes`, postfix accède beaucoup moins au disque dur. Cela n'a cependant aucune importance si l'intervalle de kupdated a été allongé.

16.5 Le paquetage powersave

Le paquetage `powersave` est responsable de l'économie d'énergie lors du fonctionnement sur batterie des ordinateurs portables. Certaines de ses caractéristiques sont toutefois aussi intéressantes pour les ordinateurs de bureau et les serveurs, par exemple, les modes veille et attente, la gestion des boutons ACPI et la mise en sommeil des disques durs IDE.

Ce paquetage rassemble toutes les fonctions de gestion d'énergie pour votre ordinateur. Il prend en charge le matériel utilisant ACPI, APM, la gestion des disques durs IDE et les technologies PowerNow! ou SpeedStep. Les fonctionnalités offertes par les paquetages `apmd`, `acpid`, `ospmd` et `cpufreqd` (maintenant,

cpuspeed) sont rassemblées dans le paquetage powersave. Il est déconseillé d'exécuter les démons de ces paquetages parallèlement au démon powersave.

Il est conseillé d'utiliser le démon powersave pour le contrôle des fonctions d'économie d'énergie, même si votre système ne comprend pas tous les éléments matériels cités précédemment. Étant donné que ACPI et APM s'excluent mutuellement, vous ne pouvez utiliser que l'un des deux sur votre système. Des modifications éventuelles de la configuration matérielle sont reconnues automatiquement par le démon.

Important

Informations sur powersave

Des informations actualisées sur le paquetage powersave sont également disponibles dans le fichier /usr/share/doc/packages/powersave.

Important

16.5.1 Configuration du paquetage powersave

D'une manière générale, la configuration de powersave est répartie sur plusieurs fichiers :

/etc/sysconfig/powersave/common
: Ce fichier contient des paramètres généraux pour le démon powersave. Entre autres, le nombre de messages de débogage (dans /var/log/messages) peut être augmenté en changeant la valeur de la variable POWERSAVE_DEBUG.

/etc/sysconfig/powersave/events
: Ce fichier est nécessaire au démon powersave pour garantir le traitement des événements (en anglais events) du système qui se produisent.
Des actions externes ou des actions que le démon traite lui-même peuvent être attribuées à un événement. On parle d'actions externes lorsque le démon essaie d'activer un fichier exécutable qui est situé dans /usr/lib/powersave/scripts/. Les actions internes prédéfinies sont :

- ignore
- throttle
- dethrottle
- suspend_to_disk
- suspend_to_ram

- standby
- do_suspend_to_disk
- do_suspend_to_ram
- do_standby

throttle ralentit le processeur de la valeur qui est définie par POWERSAVE_MAX_THROTTLING. Cette valeur est dépendante du profil utilisé actuellement. dethrottle redonne ses performances initiales au processeur. suspend_to_disk, suspend_to_ram et standby initient l'événement système pour un mode de sommeil. Ces trois dernières actions sont généralement reponsables de la mise en sommeil mais devraient toujours être soumises à des événements systèmes bien définis.

Des scripts pour le traitement d'événements se trouvent dans le répertoire /usr/lib/powersave/scripts :

notify Avertissement à travers la console, le fenêtre X ou un signal acoustique d'un événement se produisant

screen_saver Activation de l'économiseur d'écran

switch_vt Utile lorsque, après une mise en veille ou en attente, l'écran est déplacé

wm_logout Enregistrement de la configuration et déconnexion de GNOME ou KDE ou d'autres gestionnaires de fenêtre

wm_shutdown Enregistrement de la configuration GNOME ou KDE et arrêt du système

Si, par exemple, la variable POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk" est définie, les deux scripts ou actions sont traités dans l'ordre défini dès que l'utilisateur donne à powersaved l'ordre pour le mode sommeil suspend to disk. Le démon exécute le script externe /usr/lib/powersave/scripts/prepare_suspend_to_disk. Lorsque celui-ci est traité avec succès, le démon exécute l'action interne do_suspend_to_disk et met l'ordinateur définitivement en sommeil une fois que le script a arrêté les modules et les services critiques.

Une modification des actions pour l'événement d'un bouton sleep pourrait être comme dans POWERSAVE_EVENT_BUTTON_SLEEP="notify suspend_to_disk". Dans ce cas, l'utilisateur est informé de la mise en veille par le script externe notify. Ensuite, l'événement POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK est créé qui a pour suite l'exécution des actions décrites ci-dessus et garantit un mode de mise en veille sûr du

système. Le script `notify` peut être modifié dans `/etc/sysconfig/powersave/common` avec la variable `POWERSAVE_NOTIFY_METHOD`.

`/etc/sysconfig/powersave/cpufreq`
Le fichier contient des variables pour l'optimisation des paramètres dynamiques de la fréquence du processeur.

`/etc/sysconfig/powersave/battery`
Contient les limites de la batterie et d'autres paramètres spécifiques à la batterie.

`/etc/sysconfig/powersave/sleep`
Dans ce fichier, vous pouvez définir quels modules et quels services doivent être arrêtés avant que la mise en sommeil soit effectuée. Ceux-ci seront rechargés et démarrés lors de la remise en route du système. En outre, vous pouvez retarder une mise en sommeil déclenchée (pour éventuellement encore enregistrer des données). Les paramètres par défaut concernent principalement les modules USB et PCMCIA. Un échec de la mise en sommeil est généralement dû à certains modules. Consultez section 16.5.4 page 339 pour savoir comment déterminer l'erreur.

`/etc/sysconfig/powersave/thermal`
Ici, le contrôle pour la régulation de la ventilation et de la chaleur est activé. Vous trouverez plus de détails à ce sujet dans le fichier `/usr/share/doc/packages/powersave/README.thermal`.

`/etc/sysconfig/powersave/scheme_*`
Il s'agit des différents profils, qui régissent l'ajustement de la consommation d'énergie suivant des scénarios d'utilisation déterminés. Un certain nombre de profils sont préconfigurés et utilisables sans autre modification. Toutefois, vous pouvez aussi intégrer à ce fichier vos propres profils.

16.5.2 Configuration d'APM et ACPI

Mise en veille (Suspend) et mise en attente (Standby)

Par défaut, les modes de mise en sommeil sont désactivés étant donné qu'ils ne fonctionnent toujours pas sur certains ordinateurs. Il existe trois modes de mise en sommeil ACPI et deux modes APM :

Suspend to Disk (ACPI S4, APM suspend)
Enregistre le contenu entier de la mémoire sur le disque dur. L'ordinateur s'arrête complètement et n'utilise pas de courant.

Suspend to RAM (ACPI S3, APM suspend)
Enregistre l'état de tous les appareils dans la mémoire principale. Il n'y a plus que la mémoire principale qui soit alimentée en courant.

Standby (ACPI S1, APM standby) Arrête, selon le fabricant, quelques appareils.

Assurez-vous que les options par défaut suivantes sont correctement définies dans le fichier `/etc/sysconfig/powersave/events` pour un bon fonctionnement de la mise en veille, la mise en attente et de la reprise (paramètres par défaut après l'installation de SUSE LINUX) :

```
POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk do_suspend_to_disk"
POWERSAVE_EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram do_suspend_to_ram"
POWERSAVE_EVENT_GLOBAL_STANDBY=
    "prepare_standby do_standby"
POWERSAVE_EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
POWERSAVE_EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
POWERSAVE_EVENT_GLOBAL_RESUME_STANDBY=
    "restore_after_standby"
```

États de la batterie définis par l'utilisateur

Dans le fichier `/etc/sysconfig/powersave/battery`, vous pouvez définir trois niveaux de charge de la batterie (en pourcentage). Lorsque ces niveaux sont atteints, le système envoie un message d'avertissement ou exécute des opérations déterminées.

```
POWERSAVED_BATTERY_WARNING=20
POWERSAVED_BATTERY_LOW=10
POWERSAVED_BATTERY_CRITICAL=5
```

Les opérations ou scripts à exécuter lorsque la charge de la batterie descend en dessous d'un seuil donné sont définis dans le fichier de configuration `/etc/sysconfig/powersave/events`. Vous pouvez modifier les actions standard pour les boutons tel que décrit dans section 16.5.1 page 334.

```
POWERSAVE_EVENT_BATTERY_NORMAL="ignore"
POWERSAVE_EVENT_BATTERY_WARNING="notify"
POWERSAVE_EVENT_BATTERY_LOW="notify"
POWERSAVE_EVENT_BATTERY_CRITICAL="wm_shutdown"
```

Ajustement de la consommation d'énergie dans différentes conditions de travail.

Il est possible de faire dépendre le comportement du système de son alimentation électrique. Ainsi, la consommation du système devrait être réduite lorsque le système est déconnecté du réseau électrique et fonctionne sur batterie. Inversement, les performances du système devraient automatiquement revenir à un niveau élevé dès que le système est reconnecté au réseau électrique. La fréquence du processeur, la fonction d'économie d'énergie des disques durs IDE ainsi que quelques autres paramètres peuvent être modifiés.

Lors d'une connexion au réseau électrique ou de la déconnexion, l'exécution de certaines actions bien définies est spécifiée dans `/etc/sysconfig/powersave/events`. Définissez les profils à appliquer dans le fichier `/etc/sysconfig/powersave/common` :

```
POWERSAVE_AC_SCHEME="performance"
POWERSAVE_BATTERY_SCHEME="powersave"
```

Chaque profil est stocké dans un fichier lui correspondant, dans le répertoire `/etc/sysconfig/powersave`. Les noms de fichiers sont constitués de la manière suivante : `scheme_nom du profil`. Dans l'exemple ci-dessus, deux profils sont référencés : `scheme_performance` et `scheme_powersave`. Les profils `performance`, `powersave`, `presentation` et `acoustic` sont livrés préconfigurés. Vous pouvez à tout moment, au moyen du module de gestion de l'énergie de YaST (voir section 16.6 page 342), mettre en place de nouveaux profils, modifier ou supprimer des profils existants ou modifier leur affectation aux états d'alimentation électrique.

16.5.3 Autres fonctionnalités d'ACPI

Si vous êtes amené à utiliser ACPI, vous pouvez contrôler la réaction de votre système aux boutons ACPI (power, sleep, et écran ouvert, écran fermé). L'exécution des opérations correspondantes est définie dans le fichier `/etc/sysconfig/powersave/events`. Pour plus d'informations sur chacune des options, veuillez vous référer à ce fichier de configuration.

POWERSAVE_EVENT_BUTTON_POWER="wm_shutdown"
Si vous appuyez sur le bouton power, le système provoque l'extinction du gestionnaire de fenêtres (KDE, GNOME, fvwm, etc.).

POWERSAVE_EVENT_BUTTON_SLEEP="suspend_to_disk"
Si vous appuyez sur le bouton sleep, le système passe en mode veille sur disque.

POWERSAVE_EVENT_BUTTON_LID_OPEN="ignore"
L'ouverture de l'écran ne déclenche aucune action.

POWERSAVE_EVENT_BUTTON_LID_CLOSED="screen_saver"
L'économiseur d'écran est activé quand l'écran est rabattu.

Si, pendant une certaine durée, le processeur n'est pas utilisé au delà d'une certain proportion, vous pouvez réduire son activité en conséquence. Définissez le niveau en dessous duquel, dans la variable `POWERSAVED_CPU_LOW_LIMIT`, et le délai au delà duquel, dans la variable `POWERSAVED_CPU_IDLE_TIMEOUT`, l'activité du processeur est réduite.

16.5.4 Problèmes possibles et solutions

On trouve un enregistrement de chaque erreur et de chaque message d'avertissement dans le fichier `/var/log/messages`. Si vous ne trouvez à première vue aucune indication, affectez `DEBUG` dans le fichier `/etc/sysconfig/powersave/common` de façon à obtenir des messages plus détaillés. Puis incrémentez la valeur de cette variable à `7` ou même à `15` et relancez le démon. Grâce aux messages d'erreur désormais plus détaillés disponibles dans le fichier `/var/log/messages`, vous devriez être en mesure de cerner le problème. Les questions et réponses suivantes couvrent les problèmes rencontrés le plus fréquemment avec powersave.

ACPI activé avec prise en charge matérielle mais fonctionnalités non disponibles

Si vous avez des problèmes avec l'ACPI, utilisez la commande suivante pour rechercher des messages spécifiques à l'ACPI parmi les résultats de `dmesg` : `dmesg|grep -i acpi`. Pour résoudre ce problème, une mise à jour du BIOS peut s'avérer nécessaire. Consultez la page d'accueil du fabricant de votre ordinateur portable, recherchez-y une version actualisée du BIOS et installez-la sur votre système. Indiquez au fabricant de votre ordinateur qu'il doit se conformer aux dernières spécifications ACPI. Si les mêmes problèmes surviennent encore après la mise à jour du BIOS, recherchez dans les sites web suivants la dernière version de la table DSDT correspondant à votre système et remplacez dans votre BIOS la table DSDT erronée :

1. Téléchargez la DSDT correspondant à votre système à l'adresse `http://acpi.sourceforge.net/dsdt/tables`. Assurez-vous que le fichier est décompressé et compilé ; vous pouvez le vérifier avec l'extension de fichier en `.aml` (ACPI Machine Language). Si tel est bien le cas, vous pouvez passer à la troisième étape.
2. Si la table que vous avez téléchargée a pour extension de fichier `.asl` (ACPI Source Language), elle doit être compilée avec l'application iasl du paquetage `pmtools`. Exécutez à cette fin, la commande `iasl -sa fichier.asl`. La version la plus récente d'iasl (compilateur Intel ACPI) est par ailleurs disponible à l'adresse `http://developer.intel.com/technology/iapc/acpi/downloads.htm`.
3. Copiez le fichier `DSDT.aml` à l'emplacement qui vous convient (nous conseillons l'emplacement `/etc/DSDT.aml`). Éditez `/etc/sysconfig/kernel` et renseignez le chemin d'accès au fichier DSDT avec la valeur correspondante. Lancez `mkinitrd` (paquetage `mkinitrd`). Dès que vous désinstallerez votre noyau et que vous construirez un `initrd` à l'aide de `mkinitrd`, la nouvelle table DSDT sera intégrée et chargée au démarrage.

CPU Frequency ne fonctionne pas

Vérifiez, en vous basant sur les sources du noyau (`kernel-source`), si votre processeur est bien pris en charge et si vous devez éventuellement utiliser un module noyau spécifique, ou une option de module particulière, pour activer le contrôle de la fréquence du processeur. Ces informations sont disponibles dans les fichiers `/usr/src/linux/Documentation/cpu-freq/*`. Lorsqu'un module ou une option particuliers sont requis, vous devez configurer les variables `CPUFREQD_MODULE` et `CPUFREQD_MODULE_OPTS` dans le fichier `/etc/sysconfig/powersave/cpufreq`.

La mise en veille et en attente (Suspend/Standby) ne fonctionnent pas

Il existe plusieurs problèmes connus, liés au noyau, qui empêchent l'utilisation de la mise en veille ou en attente (Suspend/Standby) sur des systèmes ACPI :

- Actuellement, les systèmes dotés de plus d'1 Go de RAM ne permettent pas (encore) d'utiliser la mise en veille (Suspend).
- Les systèmes multi-processeurs ou basés sur le processeur P4 (avec hyperthreading) ne permettent pas, pour le moment, d'utiliser la mise en veille (Suspend).

Le problème peut également venir d'une implémentation défectueuse de votre DSDT (BIOS). Dans ce cas, importez une nouvelle DSDT.

Sur des systèmes ACPI et APM, s'applique ce qui suit : dès que votre système cherche à décharger des modules défectueux, l'ordinateur se bloque et l'événement de mise en veille n'est pas déclenché. Le processus inverse est également possible, si vous ne déchargez ou ne stoppez pas des modules/services qui empêchent Suspend de se réaliser. Dans les deux cas, vous devrez tenter de localiser les modules posant problème. Les fichiers de journalisation créés par le démon powersave dans `/var/log/modesommeil` sont très utiles. Si l'ordinateur ne passe pas du tout en mode sommeil, il faut en rechercher la cause dans le dernier module déchargé. Vous pouvez décharger les modules problématiques avant la mise en veille ou en attente en manipulant les paramètres suivants dans le fichier `/etc/sysconfig/powersave/sleep` :

```
POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
POWERSAVE_UNLOAD_MODULES_BEFORE_STANDBY=""
POWERSAVE_SUSPEND2DISK_RESTART_SERVICES=""
POWERSAVE_SUSPEND2RAM_RESTART_SERVICES=""
POWERSAVE_STANDBY_RESTART_SERVICES=""
```

Si vous utilisez la mise en veille ou en attente dans différents environnements de réseau ou en connexion avec des systèmes de fichiers montés distants, tels que Samba et NIS, préférez alors automounter pour monter ceux-ci ou entrez les services correspondants (par exemple, `smbfs` ou `nfs`) dans la variable citée ci-dessus. Lorsqu'un programme accède à un système de fichiers monté distant avant une mise en veille ou en attente, le service ne peut pas être arrêté correctement et le système de fichiers ne peut pas être vraiment libéré. Après la reprise du système, le système de fichiers peut être corrompu et devoir être monté à nouveau.

Utilisant ACPI, le démon Powersave ne reconnaît pas le seuil de charge de la batterie

Dans le cadre d'ACPI, le système de gestion de l'énergie peut demander au BIOS d'envoyer un message lorsqu'un seuil de charge de la batterie est franchi. L'avantage de cette méthode est qu'il n'est pas indispensable de lire en permanence l'état de charge de la batterie, ce qui réduirait les performances de l'ordinateur. Toutefois, il peut arriver que ce processus d'alerte en provenance du BIOS, qui devrait certes fonctionner, ne se déclenche en fait jamais, même en cas de franchissement de la limite de charge. Si vous observez un tel comportement sur votre système, attribuez la valeur `yes` à la variable `POWERSAVED_FORCE_BATTERY_POLLING` dans le fichier `/etc/sysconfig/powersave/battery` afin de forcer la lecture de l'état de la batterie.

16.6 Le module de gestion d'énergie de YaST

Le module Gestion d'énergie de YaST vous permet de configurer toutes les options de la gestion d'énergie décrites ci-avant. Lorsque vous lancez le module dans le Centre de contrôle de YaST avec 'Système' → 'Gestion d'énergie', le premier dialogue du module est ouvert comme dans figure 16.1 de la présente page.



FIG. *16.1: Sélection des profils*

Dans ce dialogue, sélectionnez les profils à utiliser pour le fonctionnement sur batterie et le fonctionnement sur alimentation électrique. Pour ajouter ou modifier des profils, cliquez sur 'Modifier les profils' ; ceci ouvre un aperçu des profils disponibles comme dans figure 16.2 page suivante.

Dans l'aperçu des profils, sélectionnez le profil que vous voulez modifier et cliquez sur 'Modifier'. Vous pouvez aussi créer un nouveau profil en appuyant sur le bouton 'Ajouter'. Dans les deux cas, la boîte de dialogue ouverte est identique (figure 16.3 page 344).

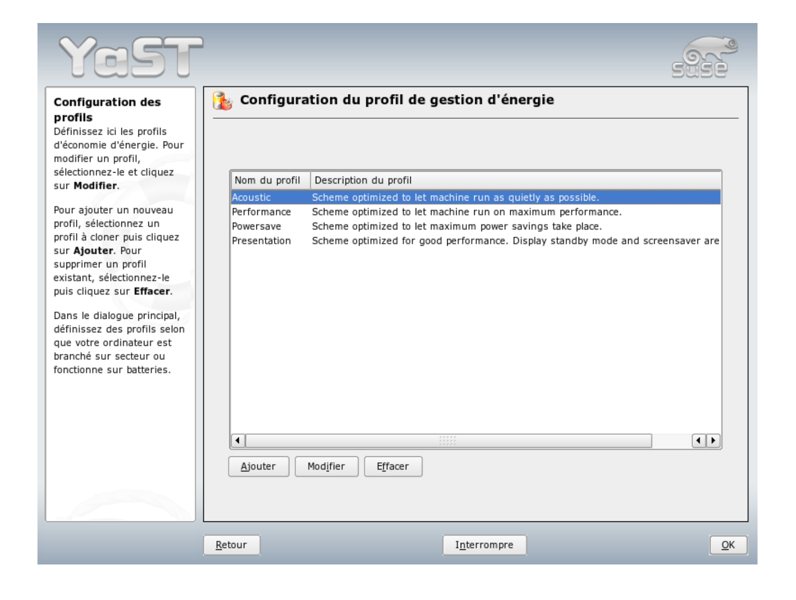


FIG. 16.2: *Aperçu des profils disponibles*

Commencez par donner au nouveau profil ou au profil modifié un nom approprié et une description. Définissez d'abord si et comment les performances du processeur doivent être réglées pour ce profil. Définissez si et à quel point le cadrage de la fréquence et le throttling doivent être utilisés. Dans le dialogue suivant, définissez les 'Règles du mode attente' qui doivent être réglées soit sur un mode de performance maximale, soit sur une consommation d'énergie minimale. Les 'Règles sonores' règlent le niveau de bruit du disque dur (ceci n'est malheureusement supporté que par peu de disques durs IDE). Les 'Règles de refroidissement' gèrent la manière dont la machine est refroidie. Malheureusement, ce type de régulation de la température n'est que rarement pris en charge par le BIOS. Veuillez consulter `/usr/share/doc/packages/powersave/README.thermal` pour savoir comment utiliser la ventilation et les méthodes de refroidissement passives. Quittez cette boîte de dialogue avec 'OK' pour activer votre configuration.

Depuis la fenêtre de démarrage, vous pouvez choisir un profil pour chaque mode de fonctionnement ainsi qu'une configuration globale de la gestion de l'énergie. Pour ce faire, cliquez sur 'Avertissements Batterie', 'Paramètres ACPI' ou 'Autori-

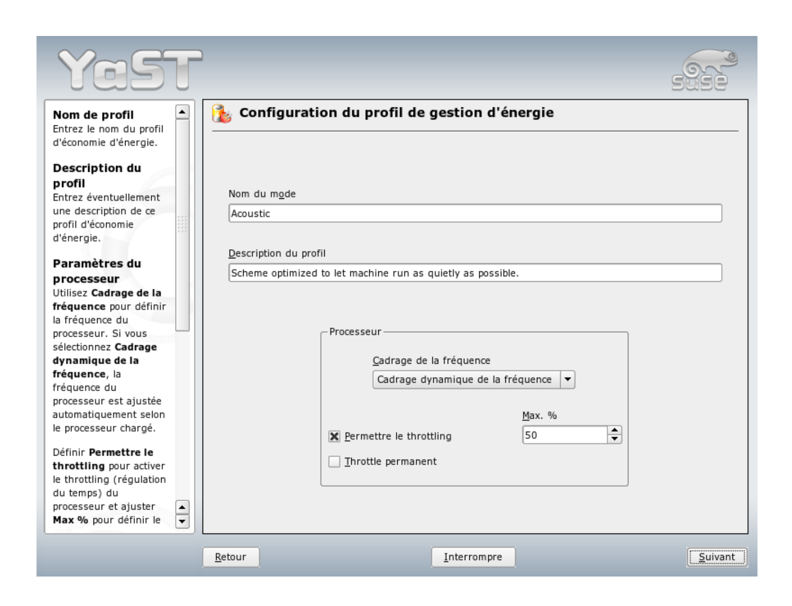


FIG. *16.3:* *Ajouter un profil*

ser la mise en veille'. Pour accéder à la boite de dialogue de l'état de charge de la batterie (figure 16.4 page suivante), cliquez sur 'Avertissements Batterie'.

Le BIOS de votre système informe le système d'exploitation lorsque certains seuils de capacité, configurables, sont atteints. Dans cette boîte de dialogue, vous pouvez fixer trois seuils en deçà desquels certaines actions doivent être déclenchées. Ce sont 'Mise en garde batterie', 'Niveau de batterie faible' et 'Niveau de batterie critique'. Dans les deux premiers cas, l'utilisateur ne recevra probablement qu'un avertissement, tandis que le passage en dessous du dernier seuil critique provoquera un arrêt de l'ordinateur, car l'énergie restante permet à peine au système de fonctionner correctement pendant un très court laps de temps. Choisissez les niveaux de charge et actions correspondant à vos souhaits et quittez la boîte de dialogue avec 'OK'. Vous revenez alors à la boite de dialogue initiale.

Vous pouvez accéder à la boîte de dialogue qui traite de la configuration des boutons ACPI avec 'Paramètres ACPI' (voir figure 16.5 page 346). Les réglages des boutons ACPI (ACPI Buttons) vous permettent de définir la réaction du système à l'utilisation des différents interrupteurs ou événements. Configurez la réponse du système à l'appui sur le bouton power, sur le bouton sleep et à la fermeture de

FIG. 16.4: *État de charge de la batterie*

l'écran du portable. Vous pouvez conclure la configuration en appuyant sur 'OK' et retourner à la boîte de dialogue initiale.

En sélectionnant 'Autoriser la mise en veille', vous ouvrez un dialogue dans lequel vous configurez si et comment un utilisateur peut utiliser les fonctionnalités de mise en veille ou en attente de ce système. Cliquez sur 'OK' pour revenir au dialogue principal. Fermez complètement le module en appuyant à nouveau sur 'OK', pour confirmer la configuration de votre gestion d'énergie.

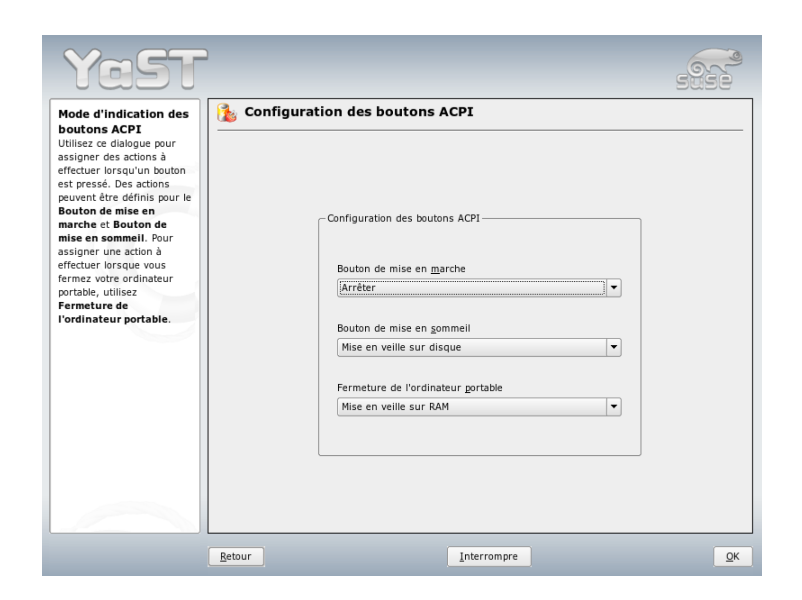


FIG. 16.5: *Réglages de l'ACPI*

Communications sans fil

Vous disposez de plusieurs possibilités pour communiquer depuis votre système Linux avec d'autres ordinateurs, des téléphones portables ou des périphériques. Si vous souhaitez mettre en réseau des ordinateurs portables, vous pouvez choisir un WLAN (Wireless LAN, réseau local sans fil). Bluetooth permet de connecter entre eux des composants système séparés (souris, clavier), des périphériques, des téléphones portables, des assistants personnels et des ordinateurs isolés. IrDA est principalement utilisé pour les communications avec des assistants personnels et des téléphones portables. Ce chapitre vous présente ces trois méthodes ainsi que leur configuration.

17.1 Réseau local sans fil (Wireless LAN)

Dans le domaine des périphériques mobiles, il n'est plus pensable de se passer des réseaux locaux sans fil (WLAN). Il n'existe pratiquement plus d'ordinateurs portables qui soient encore livrés sans carte WLAN intégrée. Le standard de transmission des cartes WLAN a été défini par l'organisation IEEE. Il s'agit du standard 802.11 qui prévoit des vitesses de transmission allant jusqu'à 2 MBit/s. Pour augmenter encore les taux de données, il a été fait depuis plusieurs ajouts. Ceux-ci définissent, entre autres, le type de modulation, le taux de transmission et, naturellement, les vitesses de transmission :

TAB. *17.1:* *Aperçu de différents standards pour WLAN*

Nom	Bande [GHz]	Taux de transfert max. [MBit/s]	Remarque
802.11	2,4	2	obsolète, il n'existe pratiquement plus de matériels d'extrémité
802.11b	2,4	11	très répandu
802.11a	5	54	peu répandu
802.11g	2,4	54	rétrocompatible avec 11b

En outre, il existe aussi des standards propriétaires tels que, par exemple, la variante 802.11b de Texas Instruments (appelé parfois 802.11b+) avec un taux de transfert maximal de 22 MBit/s. Les cartes qui utilisent ce standard sont peu répandues.

17.1.1 Matériel

Les cartes 802.11 ne sont pas prises en charge par SUSE LINUX, par contre, les cartes 802.11a, 802.11b et 802.11g sont pour la plupart prises en charge. Les cartes actuelles ont très souvent le standard 802.11g mais il existe encore des cartes 802.11b. En principe, les cartes avec les puces suivantes sont prises en charge :

- Lucent/Agere Hermes
- Intel PRO/Wireless 2100, 2200BG, 2915ABG
- Intersil Prism2/2.5/3

- Intersil PrismGT
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Texas Instruments ACX100, ACX111

Quelques cartes plus anciennes qui ne sont maintenant plus en vente mais que l'on peut encore rencontrer à quelques rares occasions sont également prises en charge. Vous trouverez une liste contenant beaucoup de cartes WLAN et les puces utilisées sur le site web de *AbsoluteValue Systems* : `http://www.linux-wlan.org/docs/wlan_adapters.html.gz` Consultez l'URL suivant pour avoir un aperçu des différentes puces WLAN : `http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz`

Certaines cartes nécessitent un micrologiciel (firmware) qui doit être chargé dans la carte lors de l'initialisation du pilote. Ceci est le cas pour Intersil PrismGT et Atmel ACX100, ACX111. Vous pouvez l'installer à l'aide de la mise en jour en ligne de YaST. Le micrologiciel pour les cartes Intel PRO-Wireless est contenu dans SUSE LINUX et est automatiquement installé par YaST dès qu'une carte de ce type est détectée. Vous trouverez plus d'informations à ce sujet dans le système installé sous `/usr/share/doc/packages/wireless-tools/README.firmware`.

Les cartes sans support Linux originel peuvent être utilisée en exécutant l'application ndiswrapper. ndiswrapper utilise les pilotes Windows qui accompagnent la plupart des cartes WLAN. Vous trouverez une description de ndiswrapper dans `/usr/share/doc/packages/ndiswrapper/README.SUSE` (à condition que le paquetage `ndiswrapper` soit installé). Consultez le site web du projet, `http://ndiswrapper.sourceforge.net/support.html`, pour obtenir des informations plus détaillées sur ndiswrapper.

17.1.2 Fonctionnement

Cette section couvre les principes fondamentaux des réseaux sans fil. Vous apprendrez ici les différents modes d'exploitation, les types d'authentification et les types de chiffrement.

Mode d'exploitation

En terme de réseaux sans fil on distingue essentiellement les réseaux gérés et les réseaux ad hoc. Les réseaux gérés comporte un élément d'administration : le point d'accès. Dans ce mode (appelé également mode infrastructure), toutes les connexions des postes de travail WLAN se trouvant dans le réseau fonctionnent

à travers le point d'accès ; celui-ci peut également servir comme interface de connexion vers un ethernet. Les réseaux ad hoc ne comportent pas de point d'accès, les postes de travail communiquent directement les uns avec les autres. La portée et le nombre de postes de travail étant très limités dans les réseaux ad hoc, il est généralement préférable d'utiliser un point d'accès. Il est même possible d'utiliser une carte WLAN comme point d'accès car la plupart supporte cette fonctionnalité.

Étant donné qu'un réseau sans fil est beaucoup plus vulnérable qu'un réseau câblé, des méthodes d'authentification et de chiffrement sont prévues dans les différents standards. Dans la première version du standard IEEE 802.11, ces méthodes sont décrites sous le terme WEP. Cependant, comme il s'est avéré que WEP n'était pas sûr (voir la section Sécurité page 355), l'industrie WLAN (unie sous le nom *Wi-Fi Alliance*) a défini son propre complément du standard nommé WPA qui devait éliminer les points faibles de WEP. Le standard IEEE 802.11i plus récent (parfois également nommé WPA2, WPA étant en fait inspiré d'une ébauche de 802.11i) comporte le dispositif de sécurité WPA ainsi que quelques méthodes d'authentification et de chiffrement supplémentaires.

Authentification

Dans les réseaux gérés, différents mécanismes d'authentification sont utilisés pour s'assurer que seuls les postes de travail autorisés puissent se connecter :

Open Un système est dit ouvert (en anglais open) lorsqu'il n'est procédé à aucune authentification. Chaque poste de travail peut entrer dans le réseau. Cependant, une methode de chiffrement conforme à WEP (voir la section Chiffrement page ci-contre) peut être utilisée.

Clé partagée (selon IEEE 802.11) Ici, la clé WEP est utilisée pour l'authentification. Cependant, cela ne devrait pas être fait car cela rend la clé WEP plus vulnérable. Il suffit à un intrus potentiel d'"épier" suffisamment longtemps la communication entre le poste de travail et le point d'accès ; les deux échangent les mêmes informations lors du processus d'authentification, une fois chiffrée et une fois en clair ; avec les outils appropriés, on peut alors reconstruire la cle utilisée. Étant donné que, dans ce système, la clé WEP est utilisée aussi bien pour l'authentification que pour le chiffrement, la sécurité du réseau n'est pas améliorée. Un poste de travail qui est en possession de la clé WEP correcte peut à la fois s'authentifier et chiffrer et déchiffrer. Un poste de travail qui n'est pas en possession de la clé WEP correcte échouera, au plus tard, lorsqu'il s'agira de déchiffrer les paquets reçus. Il ne peut donc pas communiquer, qu'il ait à s'authentifier ou non.

WPA-PSK (selon IEEE 802.1x) WPA-PSK (PSK pour Pre-Shared Key, clé pré-partagée) fonctionne de la même façon que dans le cas de la clé partagée. Tous les postes de travail participants ainsi que le point d'accès nécessitent la même clé. Celle-ci a une longueur de 256 bits et est normalement entrée comme une phrase d'authentification. Ce système ne nécessite pas une gestion complexe des clés comme c'est le cas pour WPA-EAP et est plutôt conçu pour une utilisation privée. WPA-PSK est donc appelé quelquefois aussi WPA "Home".

WPA-EAP (selon IEEE 802.1x) En fait, WPA-EAP n'est pas un système d'authentification mais seulement un protocole de transport des informations nécessaires à l'authentification. Il est utilisé au sein des entreprises pour la sécurisation des réseaux sans fil. Dans les réseaux privés, il est pratiquement inutilisé. WPA-EAP est donc appelé quelquefois aussi WPA "Enterprise".

Chiffrement

Afin de s'assurer qu'aucun tiers non autorisé puisse lire les paquets de données échangés dans un réseau sans fil ou même accéder au réseau, il existe différentes méthodes de chiffrement :

WEP (défini dans IEEE 802.11) Ce standard utilise l'algorithme de chiffrement RC4, avec une clé de 40 bits à l'origine puis avec une clé de 104 bits aussi. Souvent, on parle de longueurs de 64 ou 128 bits selon que l'on tient compte ou non des 24 bits du vecteur d'initialisation. Cependant, ce standard a des points faibles. Il existe des méthodes d'attaque des clés générées par ce système qui fonctionnent. Néanmoins, il est préférable d'utiliser WEP qu'un réseau sans chiffrement.

TKIP (défini dans WPA/IEEE 802.11i)
Ce protocole de gestion des clés défini dans le standard WPA utilise le même algorithme de chiffrement que WEP en palliant à ses faiblesses. Étant donné que, pour chaque paquet de données, une nouvelle clé est générée, les attaques de cette clé n'ont pratiquement aucune chance de réussir. TKIP est utilisé avec WPA-PSK.

CCMP (défini dans IEEE 802.11i) CCMP décrit la gestion des clés. Ce protocole est normalement utilisé avec WPA-EAP mais peut également être utilisé avec WPA-PSK. Le chiffrement est fait ici selon AES et est plus fiable que le chiffrement RC4 du standard WEP.

17.1.3 Configuration avec YaST

Pour la configuration de votre carte réseau sans fil, démarrez le module de YaST 'Carte réseau'. Dans le dialogue 'Configuration des adresses réseau', sélectionnez le type de périphérique 'sans fil' et cliquez sur 'Suivant'.



FIG. 17.1: *Configuration YaST de la carte réseau sans fil*

Dans le dialogue 'Configuration de la carte réseau sans fil' décrit dans la figure 17.1 de la présente page, procédez à la configuration de base pour l'exploitation WLAN :

Mode d'exploitation Il existe trois diffétents modes selon lesquels votre poste de travail peut être intégré dans un WLAN. Le mode approprié à votre cas dépend du type de réseau dans lequel vous désirez communiquer : 'ad hoc' (réseau pair à pair pur sans point d'accès), 'géré' (réseau géré depuis un point d'accès) et 'maître' (carte réseau à utiliser comme point d'accès).

Nom de réseau (ESSID) Tous les postes de travail d'un réseau sans fil nécessitent le même ESSID afin de pouvoir communiquer. Si rien n'a été précisé, la carte recherche automatiquement un point d'accès qui n'est peut-être pas celui que vous souhaitiez utiliser.

Mode d'authentification Choisissez une méthode d'authentification appropriée à votre réseau : 'Ouvert', 'Clé partagée WEP' ou 'WPA-PSK'. Si vous choisissez 'WPA-PSK', vous devrez définir un nom de réseau.

Paramètres pour experts Avec ce bouton, vous ouvrez un dialogue pour la configuration détaillée de votre accès WLAN. Vous trouverez, plus loin, une description détaillée de ce dialogue.

Une fois que vous avez terminé la configuration de base, votre poste de travail est prêt pour l'utilisation dans un WLAN.

Important

Sécurité dans un réseau sans fil

Veillez à utiliser une des méthodes d'authentification et de chiffrement prises en charge afin de sécuriser votre réseau. Les connexions WLAN non chiffrées permettent à des tiers d'accéder sans encombres à toutes les données du réseau. Même une méthode de chiffrement faible (WEP) est préférable à rien du tout. En cas de doute, veuillez lire la section Chiffrement page 351 et la section Sécurité page 355 pour plus d'informations.

Important

Selon la méthode d'authentification choisie, YaST vous propose, dans un autre dialogue, de procéder à des réglages fins de la méthode en question. Si vous avez choisi 'Ouvert', il n'y a rien d'autre à configurer, étant donné que ce choix suppose une exploitation non chiffrée et sans authentification.

Clés WEP Définissez le type d'entrée de la clé. Vous avez le choix entre 'Phrase d'authentification', 'ASCII' ou 'Hexadécimal'. Vous pouvez avoir jusqu'à quatre clés différentes pour chiffrer les données transférées. Cliquez sur 'Clés multiples' pour entrer dans le dialogue de configuration. Définissez la longueur de la clé. Vous avez le choix entre '128 bits' et '64 bits'. La configuration par défaut est '128 bits'. La liste sous le dialogue peut comporter jusqu'à quatre clés différentes que votre poste de travail peut employer pour le chiffrement. Avec 'Défini par défaut', définissez une de ces clés comme la clé par défaut. Si vous ne le faites pas, YaST considérere la première clé comme étant la clé par défaut. Si vous effacez la clé par défaut, vous devrez sélectionner manuellement une des clés restantes comme par clé par défaut. Utilisez 'Modifier' pour changer les entrées de la liste ou ajouter de nouvelles clés. Un menu contextuel vous permet de choisir parmi différents types d'entrée ('Phrase d'authentification', 'ASCII' ou 'Hexadécimal'). Si

vous choisissez le type d'entrée 'Phrase d'authentification', saisissez un mot ou une chaîne de caractères à partir de quoi une clé de la longueur définie précédemment sera générée. Avec 'ASCII', vous devrez entrer cinq caractères pour une longueur de clé de 64 bits et treize caractères pour une longueur de clé de 128 bits. Si vous avez choisi le type d'entrée 'Hexadécimal', entrez dix caractères hexadécimaux pour une longueur de clé de 64 bits et 26 caractères hexadécimaux pour une longueur de clé de 128 bits.

WPA-PSK Pour entrer une clé pour WPA-PSK, choisissez le type d'entrée 'Phrase d'authentification' ou 'Hexadécimal'. Dans le mode 'Phrase d'authentification', l'entrée doit comprendre entre huit et 63 caractères ; dans le mode 'Hexadécimal', l'entrée doit comprendre 64 caractères.

Avec 'Paramètres pour experts', vous passez du dialogue de configuration de base de l'accès WLAN au dialogue de configuration pour experts. Vous disposez des options suivantes :

Canal La spécification d'un canal particulier que votre poste de travail WLAN doit utiliser n'est nécessaire que dans les modes 'ad hoc' et 'maître'. Dans le mode 'géré', la carte recherche automatiquement les points d'accès dans les canaux disponibles. Dans le mode 'ad hoc', vous pouvez sélectionner l'un des douze canaux offerts pour que votre poste de travail communique avec les autres postes de travail. Dans le mode 'maître', définissez sur quel canal votre carte doit offrir le service de point d'accès. La configuration par défaut de cette option est 'auto'.

Débit binaire Selon les performances de votre réseau, il est utile de prédéfinir un débit binaire avec lequel les données doivent être transmises d'un point à un autre. Dans la configuration par défaut 'auto', votre système utilise la vitesse de transmission la plus rapide possible. Veuillez noter que la configuration du débit binaire n'est pas prise en charge par toutes les cartes WLAN.

Point d'accès Dans un environnement avec plusieurs points d'accès, vous pouvez en présélectionner un ici en entrant son adresse MAC.

Utiliser la gestion d'énergie Si vous êtes en déplacement, il est conseillé d'augmenter la durée d'utilisation des batteries grâce à des techniques d'économie d'énergie. Pour en savoir plus sur la gestion d'énergie sous Linux, veuillez lire le chapitre 16 page 321.

17.1.4 Utilitaires

hostap (paquetage `hostap`) est utilisé pour exploiter une carte WLAN comme un point d'accès. Vous trouverez plus d'informations relatives à ce paquetage sur le site web du projet (`http://hostap.epitest.fi/`).

kismet (paquetage `kismet`) est un outil de diagnostic du réseau avec lequel vous pouvez surveiller le transfert de paquets WLAN ou même l'épier et ainsi déceler des tentatives d'intrusion dans votre réseau. Vous trouverez plus d'informations à ce sujet sous `http://www.kismetwireless.net/` ou dans les pages de manuel correspondantes.

17.1.5 Trucs et astuces pour la configuration d'un WLAN

Vous apprendrez ici comment peaufiner la vitesse et la stabilité ainsi que les aspects de sécurité de votre réseau WLAN.

Stabilité et vitesse

La performance et la fiabilité d'un réseau sans fil dépendent tout d'abord de la netteté du signal que se transmettent les postes de travail qui appartiennent au réseau. Bien entendu, les obstacles, tels que des murs, affaiblissent considérablement le signal. Plus le signal est faible, plus la vitesse de transfert diminue. Vous pouvez vérifier la force du signal pendant le fonctionnement avec le programme iwconfig à la ligne de commande (champ 'Link Quality') ou kwifimanager sous KDE. Si vous avez des problèmes avec la qualité du signal, essayez de placer autrement les appareils ou de changer l'angle de l'antenne de votre point d'accès. Pour certaines cartes WLAN PCMCIA, il existe des antennes supplémentaires qui améliorent considérablement la réception. La vitesse donnée par le fabricant (par exemple 54 MBit/s) est toujours une valeur nominale. Il ne s'agit que du maximum théorique. En pratique, la vitesse de transfert atteint au mieux la moitié de cette valeur.

Sécurité

Lorsque vous souhaitez configurer un réseau sans fil, pensez que, sans mesures de sécurité particulières, votre réseau est facilement accessible à tous ceux se trouvant à sa portée. Activez donc, dans tous les cas, une méthode de chiffrement. Chaque périphérique d'extrémité, qu'il s'agisse d'une carte WLAN ou d'un point d'accès, prend en charge le chiffrement selon le protocole WEP. Ceci

n’est pas absolument sûr mais cela représente tout de même une certaine protection contre les attaques potentielles. Pour une utilisation privée, WEP est généralement suffisant. Il serait encore préférable d’utiliser WPA-PSK. Cependant, cette méthode n’est pas implémentée dans les points d’accès ou les routeurs avec fonctionnalité WLAN plus anciens. Pour certains, il est possible d’implémenter WPA en procédant à une mise à jour avec un micrologiciel (firmware), mais pas pour tous. Même Linux n’assure pas la prise en charge de WPA sur tous les matériels. À l’heure où nous rédigeons ce chapitre, WPA ne fonctionne qu’avec les cartes qui utilisents une puce Atheros ou Prism2/2.5/3 ; et pour cette dernière, uniquement lorsque le pilote hostap est utilisé (voir la section Problèmes avec cartes Prism2 de la présente page). Cependant, dans les cas où il n’est pas possible d’utiliser WPA, il est toujours préférable d’utiliser WEP qu’aucune méthode de chiffrement. Au sein d’une entreprise où les exigences en matière de sécurité sont plus importantes, un réseau sans fil ne devrait jamais être utilisé sans WPA.

17.1.6 Problèmes possibles et solutions

Si votre carte WLAN ne fonctionne pas, assurez-vous que vous avez téléchargé le micrologiciel (firmware) nécessaire. Consultez la section 17.1.1 page 348. Les paragraphes suivants traitent de quelques problèmes connus.

Plusieurs périphériques réseau

Les portables actuels sont normalement équipés d’une carte réseau et d’une carte WLAN. Si vous avez configuré ces deux périphériques avec DHCP (assignation automatique d’adresse), vous pourrez éventuellement avoir des problèmes avec la résolution de noms et la passerelle par défaut. Vous pourrez alors faire un ping sur le routeur mais vous ne pourrez pas surfer sur Internet. Il existe un article SDB à ce sujet, recherchez le mot-clé ”DHCP“ dans la base de données support sur `http://portal.suse.com`.

Problèmes avec cartes Prism2

Pour les périphérique équipés de puces Prism2, il existe plusieurs pilotes qui fonctionnent plus ou moins bien avec les différentes cartes. Avec ces cartes, WPA n’est possible qu’avec le pilote hostap. Si vous avez des problèmes avec une telle carte, qu’elle ne fonctionne pas du tout ou que de façon sporadique ou que vous voulez utiliser WPA, veuillez lire `/usr/share/doc/packages/wireless-tools/README.prism2`.

WPA

La prise en charge de WPA a été implémentée pour la première fois par SUSE LINUX. Sous Linux, la prise en charge WPA n'est pas encore arrivée complètement à maturité. Ainsi, vous ne pouvez, avec YaST, configurer que WPA-PSK. WPA ne fonctionne pas avec de nombreuses cartes. Certaines nécessitent une mise à jour du micrologiciel (firmware) pour que WPA puisse fonctionner. Si vous souhaitez utiliser WPA, veuillez lire `/usr/share/doc/packages/wireless-tools/README.wpa`.

17.1.7 Informations complémentaires

Vous trouverez une mine d'informations utiles au sujet des réseaux sans fil sur les pages web de Jean Tourrilhes qui a développé les *Wireless Tools* pour Linux : `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html`

17.2 Bluetooth

Bluetooth est une technologie radio qui permet de connecter plusieurs appareils entre eux : téléphones mobiles, PDA, périphériques ou composants système tels que clavier ou souris, ordinateurs portables. Le nom provient du roi danois Harold Blatand ("Harold Bluetooth" en anglais) qui a unifié au dixième siècle différentes factions se combattant entre elles en Scandinavie. Le logo de Bluetooth est basé sur les runes représentant les lettres "H" (qui ressemble à une étoile) et "B".

Bluetooth se distingue de l'IrDA en plusieurs points essentiels : d'une part, les différents appareils n'ont pas besoin de se "voir" directement pour échanger des données, d'autre part il est possible de mettre au point des réseaux entiers en rassemblant plusieurs appareils. Cette technologie ne permet toutefois d'atteindre que des débits de 720 Kbit/s maximum (dans la version 1.1 actuelle). En théorie, on peut, avec Bluetooth, envoyer des données par radio à travers les murs. Dans la pratique, cela dépend fortement des murs en question et du type des appareils. Enfin, la portée maximale d'envoi est répartie en trois classes qui varient de dix à cent mètres.

17.2.1 Principes de base

Les sections suivantes présentent les principes de base du fonctionnement de Bluetooth. Vous y apprendrez à quels besoins logiciels vous devez satisfaire,

quelles sont les interactions de Bluetooth avec votre système et comment les profils Bluetooth fonctionnent.

Logiciels

Pour pouvoir utiliser Bluetooth, vous avez besoin d'un adaptateur Bluetooth (intégré à l'appareil ou sous la forme d'une périphérique externe), de pilotes et de ce que l'on appelle une "pile de protocoles Bluetooth". Le noyau Linux contient déjà les pilotes de base permettant d'utiliser Bluetooth. On utilise comme pile de protocoles le système Bluez. Afin que les différentes applications puissent fonctionner avec Bluetooth, vous devez, en outre, installer les paquetages de base suivants : `bluez-libs` et `bluez-utils` qui préparent quelques services et utilitaires nécessaires. Pour quelques adaptateurs (Broadcom, AVM BlueFritz!), il est par ailleurs nécessaire d'installer `bluez-firmware`. Le paquetage `bluez-cups` permet l'impression via une connexion Bluetooth.

Interaction générale

Un système Bluetooth est constitué de quatre couches imbriquées de manière à fournir en bout de chaîne les fonctions souhaitées :

Matériel L'adaptateur et le pilote approprié qui assure la prise en charge par le noyau Linux.

Fichiers de configuration Le paramétrage du système Bluetooth

Démons Services qui, par l'intermédiaire des commandes du fichier de configuration, mettent à disposition les fonctionnalités.

Applications Programmes qui permettent à l'utilisateur d'utiliser et de piloter les fonctionnalités mises à disposition par les démons.

À l'insertion de l'adaptateur Bluetooth, le pilote correspondant est chargé par le système Hotplug. Une fois le pilote chargé, les fichiers de configuration permettent de vérifier si Bluetooth doit être démarré. Si tel est le cas, le système détermine également quels services doivent être démarrés. Les démons correspondants sont alors lancés en conséquence. Les adaptateurs Bluetooth sont recherchés lors de l'installation. Si un ou plusieurs sont trouvés, Bluetooth est activé. Sinon, le système Bluetooth est désactivé. Chaque périphérique Bluetooth ajouté ultérieurement doit être activé manuellement.

Profils

Dans Bluetooth, les services sont définis au moyen de ce que l'on appelle des profils. On définit ainsi dans le standard Bluetooth des profils pour le transfert de données ("File Transfer"), l'impression ("Basic Printing") et les connexions réseau ("Personal Area Network"). Pour qu'un appareil puisse utiliser le service d'un autre, ces deux appareils doivent pouvoir comprendre le même profil—information qui, souvent, n'est malheureusement disponible ni sur l'emballage ni dans le manuel des appareils concernés. Cela est d'autant plus compliqué que tous les fabricants ne respectent pas scrupuleusement les définitions des différents profils. En règle générale toutefois, la compréhension entre les appareils fonctionne plutôt bien.

Dans le texte qui suit, les périphériques locaux sont ceux connectés physiquement à l'ordinateur. Tous les autres périphériques auxquels on ne peut accéder qu'à travers des connexions sans fil sont appelés des périphériques distants.

17.2.2 Configuration

Cette section présente la configuration Bluetooth. Vous y apprendrez quels sont les fichiers de configuration impliqués, quels outils sont nécessaires et comment configurer Bluetooth à l'aide de YaST ou manuellement.

Configuration Bluetooth avec YaST

Avec le module Bluetooth de YaST, tel que dans la figure 17.2 page suivante, vous pouvez configurer la prise en charge de Bluetooth sur votre système. Dès que Hotplug reconnaît un adaptateur Bluetooth connecté à votre système (par exemple, lors de l'amorçage ou si vous enfichez un adaptateur), Bluetooth est automatiquement démarré suivant les paramètres configurés dans ce module.

La première étape de la configuration vous permet de définir si des services Bluetooth doivent être démarrés sur votre système. Si vous avez activé les services Bluetooth, vous pouvez configuré deux choses. Tout d'abord, le 'Nom de périphérique'. Ceci est le nom que d'autres périphériques affichent lorsque votre ordinateur a été détecté. Il y a deux marques de réservation possibles—`%h` symbolise le nom d'hôte du système (utile, par exemple, s'il est assigné dynamiquement par DHCP) et `%d` insère le numéro d'interface (utile uniquement si vous il y a plus d'un adaptateur Bluetooth dans votre ordinateur). Par exemple, si vous entrez `Laptop %h` dans le champ de saisie et si DHCP assigne le nom `unit123` à votre ordinateur, d'autres périphériques distants reconnaitront votre ordinateur comme `Laptop unit123`.

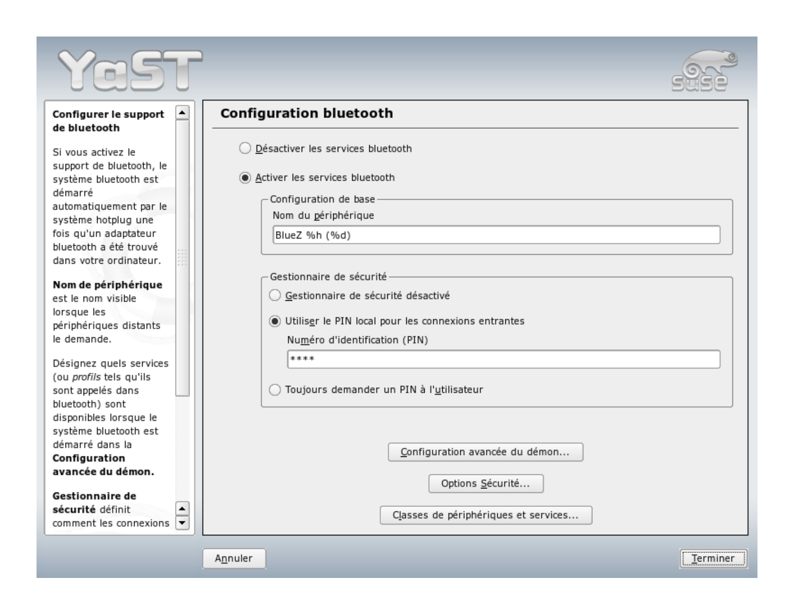


FIG. 17.2: *Configuration Bluetooth dans YaST*

Le second paramètre 'Gestionnaire de sécurité' est lié au comportement du système local lorsqu'un périphérique distant essaie de se connecter. La différence réside dans le traitement du numéro d'identification (pin). Soit vous autorisez tout périphérique à se connecter sans PIN, soit vous définissez comment le PIN correct est choisi s'il est nécessaire. Vous pouvez entrer un PIN (enregistré dans un fichier de configuration) dans le champ de saisie correspondant. Si un périphérique essaie de se connecter, il utilise d'abord ce PIN. Si cela ne fonctionne pas, il n'utilise pas de PIN. Pour assurer un sécurité maximale, il est préférable de choisir la troisième option, "Toujours demander le PIN". Cette option vous permet d'utiliser des PIN différents pour des périphériques (distants) différents.

Cliquez sur le bouton 'Configuration avancée du démon' pour entrer dans le dialogue de sélection et de configuration des services proposés (également connus dans Bluetooth sous le nom de *Profils*). Tous les services à votre disposition sont donnés dans une liste, et les boutons 'Activer' et 'Désactiver' permettent d'effectuer sur chaque service l'opération correspondante. Le bouton 'Modifier' ouvre une nouvelle fenêtre dans laquelle vous pouvez fournir des arguments supplémentaires au service (démon) sélectionné. N'effectuez des modifications que dans

les services que vous connaissez suffisamment bien. Lorsque la configuration du démon est terminée, vous quittez la boîte de dialogue en cliquant sur 'OK'.

De retour dans la fenêtre principale, vous ouvrez un dialogue de configuration de la sécurité en cliquant sur 'Options Sécurité' qui vous permet de configurer les paramètres de chiffrement, d'authentification et de balayage. Fermez la fenêtre de configuration de la sécurité pour retourner à la boîte de dialogue principale. Quittez celle-ci en cliquant sur le bouton 'Terminer', votre système Bluetooth est prêt à être utilisé.

Depuis le dialogue principal, vous pouvez aussi atteindre le dialogue 'Classes de périphériques et services'. Les périphériques Bluetooth sont groupés dans différentes "Classes de périphériques". Dans ce dialogue, faites la sélection correcte pour votre ordinateur, par exemple "Bureau" ou "Portable". La classe de périphériques n'est pas très importante contrairement à la "Classe de services" définie également ici. Quelquefois, des périphériques Bluetooth distants, tels que des téléphones portables, ne permettent certaines fonctions que s'ils peuvent détecter la classe de services correcte définie sur votre système. Ceci est souvent le cas de téléphones portables qui exigent une classe appelée "Transfert d'objet" avant de permettre le transfert de fichiers depuis ou vers l'ordinateur. Vous pouvez choisir des classes multiples. Il n'est pas utile de sélectionner toutes les classes "juste au cas où". Dans la plupart des cas, la sélection par défaut devrait suffire.

Pour utiliser Bluetooth dans la construction d'un réseau, activez 'PAND'dans la boîte de dialogue 'Configuration Avancée du Démon' puis, en choisissant 'Modifier', ajustez le mode du démon. Pour que la connexion réseau Bluetooth fonctionne, il est nécessaires qu'une instance de pand fonctionne en mode 'Ecoute' et que le récepteur soit en mode 'Recherche'. Par défaut, le mode 'Ecoute' est préconfiguré. Ajustez le comportement de votre instance locale de pand. De plus, vous pouvez, au moyen du module 'Carte réseau' de YaST, configurer l'interface `bnepX` (`X` représente le numéro du périphérique dans le système).

Configuration manuelle de Bluetooth

Les fichiers de configuration pour les composants individuels du système Bluez se trouvent dans le répertoire `/etc/bluetooth`. La seule exception à cette règle est le fichier `/etc/sysconfig/bluetooth` pour le démarrage des composants modifié par le module de YaST.

Vous ne pouvez modifier les fichiers de configuration présentés ci-après qu'en tant qu'utilisateur `root`. Il n'existe pour l'instant malheureusement pas encore d'interface utilisateur graphique pour changer *tous* les paramètres. Les plus importants peuvent être définis à l'aide du module Bluetooth de YaST décrit dans la

section Configuration Bluetooth avec YaST page 359. Tous les autres paramètres ne sont relevants que pour des utilisateurs expérimentés dans des cas spéciaux. Toutefois, en règle générale, les réglages d'origine devraient suffire.

Une première protection contre les connexions indésirables consiste à utiliser une protection par un numéro d'identification personnel (PIN). Les téléphones portables demandent généralement à l'utilisateur de saisir son numéro d'identification personnel lors du premier contact (ou de la création d'un contact pour l'appareil sur le téléphone). Pour que deux appareils puissent échanger des informations, ils doivent tous les deux s'identifier avec le même numéro d'identification personnel. Ce dernier se trouve dans le fichier `/etc/bluetooth/pin` sur l'ordinateur.

Important

Sécurité des connexions Bluetooth

Malgré le numéro d'identification personnel, il faut garder à l'esprit qu'une connexion entre deux appareils n'est absolument pas garantie contre les écoutes. Prenez garde au fait qu'en mode d'émission, l'authentification et le chiffrement des connexions Bluetooth sont désactivées. Activer l'authentification et le chiffrement peut causer des problèmes de communication avec certains périphériques Bluetooth.

Important

Le fichier de configuration `/etc/bluetooth/hcid.conf` permet de modifier différents paramètres tels que les noms des périphériques et le mode de sécurité. Normalement, les réglages par défaut doivent suffire. Le fichier contient des commentaires qui décrivent les options des différents paramètres. Nous évoquons ici rapidement deux réglages particuliers.

Dans le fichier fourni se trouvent deux sections désignées par `options` et `device`. La première contient toutes les informations générales utilisées au démarrage d'hcid, la seconde contient les réglages pour les périphériques Bluetooth locaux individuels.

L'un des réglages les plus importants de la partie `options` est `security auto;`. Il permet d'activer la nécessité d'un numéro d'identification personnel. `auto`, en cas de problème, permet de passer à `none` (pas de numéro d'identification personnel nécessaire) et d'établir la connexion dans tous les cas. Pour un niveau de sécurité plus élevé, il est conseillé de régler cet élément sur `user`, de façon à ce que l'utilisateur doive fournir un numéro d'identification personnel à chaque connexion.

La section `device` est intéressante car elle permet de définir le nom sous lequel l'ordinateur apparaît face à ses correspondants. Les classes des appareils, telles que `Desktop` (ordinateur de bureau), `Laptop` (ordinateur portable) et `Server` (serveur), sont également définis ici, ainsi que l'authentification et le chiffrement.

17.2.3 Composants système et utilitaires

Ce n'est qu'après avoir combiné plusieurs services que Bluetooth peut véritablement être utilisé. Vous avez besoin d'au moins deux démons à exécuter en tâche de fond : d'une part, hcid (*host controller interface*) qui sert d'interface avec l'appareil Bluetooth et le pilote et d'autre part, sdpd (*service discovery protocol*). sdpd permet à un appareil de découvrir quels services l'ordinateur propose. Aussi bien hcid que sdpd peuvent, si cela ne se produit pas déjà automatiquement lors du démarrage du système, être mis en service avec la commande `rcbluetooth start`. Cependant, cette commande doit être exécutée par l'utilisateur `root`.

Dans la suite nous traiterons brièvement des plus importants outils en mode ligne de commande qui peuvent être utilisés pour travailler avec Bluetooth. Même si Bluetooth peut être utilisé par le biais de différents composants graphiques, nous vous recommandons de jeter un œil à ces programmes.

Certaines commandes ne peuvent être lancées qu'en tant qu'utilisateur `root`. C'est le cas de `l2ping` ⟨*device_address*⟩ qui permet de tester la connexion avec un périphérique distant.

hcitool

hcitool permet de déterminer facilement si des périphériques locaux et des périphériques distants ont été détectés. La commande `hcitool dev` permet d'afficher les périphériques locaux. Le résultat génère, pour chaque périphérique local trouvé, une ligne de la forme suivante : ⟨*nom-interface*⟩ ⟨*adresse-périphérique*⟩.

Utilisez la commande `hcitool inq` pour rechercher des périphériques distants. Vous obtenez ici trois valeurs par périphérique trouvé : l'adresse du périphérique, le décalage horaire et la classe du périphérique. La plus importante est l'adresse du périphérique. Elle est utilisée par d'autres commandes pour identifier le périphérique cible. La décalage horaire n'est normalement intéressant que d'un point de vue technique. Dans la classe, le type de périphérique et le type de service sont codés en valeur hexadécimale.

Vous pouvez utiliser la commande `hcitool name` ⟨*adresse-périphérique*⟩ pour obtenir le nom d'un appareil distant. S'il s'agit alors d'un ordinateur dis-

tant, la classe et le nom de l'appareil obtenus correspondent alors aux informations contenues dans le fichier `/etc/bluetooth/hcid.conf` de celui-ci. Les adresses d'appareils locaux génèrent une erreur en sortie.

hciconfig

`/usr/sbin/hciconfig` fournit des informations supplémentaires pour les périphériques locaux. L'appel de `hciconfig` sans argument fournit des informations sur le périphérique comme le nom du périphérique (`hciX`), l'adresse physique du périphérique (12 chiffres sous la forme `00:12:34:56:78`) ainsi que des informations sur la quantité de données transmises.

`hciconfig hci0 name` renvoie le nom qui est renvoyé par votre ordinateur à toute demande d'appareils distants.`hciconfig` ne sert cependant pas qu'à répondre aux requêtes des appareils vers l'appareil local, mais permet également de modifier les paramètres. La commande `hciconfig hci0 name TEST` permet de donner à l'appareil le nom `TEST`.

sdptool

Utilisez le programme sdptool pour savoir quel service est mis à disposition par un appareil donné. La commande `sdptool browse` ⟨*adresse_périphérique*⟩ fournit une liste de tous les services d'un appareil, tandis que `sdptool search` ⟨*code_service*⟩ permet de rechercher un service donné. Cet appel interroge tous les appareils qui peuvent être joints pour leur demander s'ils proposent le service recherché. S'il est effectivement proposé par un appareil, le programme indique le nom du service complet proposé par l'appareil et une brève description. Pour obtenir une liste de tous les codes de services possibles, exécutez la commande `sdptool` sans paramètre particulier.

17.2.4 Applications graphiques

Konqueror vous permet d'afficher la liste des périphériques Bluetooth locaux et distants grâce à l'URL `bluetooth:/`. Un double clic sur le périphérique vous affiche une vue d'ensemble des services proposés par ce périphérique. Si vous passez la souris sur un des services fournis, vous pouvez voir dans la barre d'état du navigateur le profil utilisé pour ce service. Cliquez sur un service, une fenêtre apparaît alors pour vous demander ce que vous désirez faire : enregistrer, utiliser le service (il faut pour cela qu'un programme utilisateur soit lancé) ou annuler votre

action. Vous pouvez aussi cocher une case pour que cette fenêtre ne s'affiche plus mais exécute toujours une action que vous aurez choisie. Attention : pour certains services il n'existe pas encore de prise en charge, et pour d'autres des paquetages supplémentaires doivent éventuellement être installés.

17.2.5 Exemples

Cette section présente deux exemples typiques de scénarios Bluetooth possibles. Le premier montre comment une connexion réseau entre deux hôtes peut être établie via Bluetooth. Le second montre une connexion entre un ordinateur et un téléphone portable.

Connexion réseau entre deux ordinateurs

Dans le premier exemple, on doit construire une connexion réseau entre deux ordinateurs *O1* und *O2*. Chacun des deux ordinateurs possède une adresse de périphérique Bluetooth, respectivement *baddr1* et *baddr2*, laquelle, comme il a été décrit ci-dessus, peut être définie à l'aide de la commande `hcitool dev` sur chaque ordinateur. Les ordinateurs doivent être identifiés par leur adresse IP respective soit `192.168.1.3` (*O1*) et`192.168.1.4` (*O2*).

La connexion Bluetooth a lieu grâce à pand (personal area networking). Les commandes suivantes doivent être lancées par l'utilisateur `root`. Nous omettons délibérement toute explication détaillée de la commande réseau `ip` pour nous concentrer sur les actions propres à Bluetooth :

Sur l'ordinateur *O1*, on démarre pand avec la commande `pand -s`. Sur le deuxième ordinateur *O2*, on peut alors construire une connexion avec la commande `pand -c` ⟨*baddr1*⟩. Si vous demandez maintenant, sur l'un ou les deux ordinateurs, une liste des interfaces réseau à disposition, avec la commande `ip link show`, vous devez obtenir une réponse de la forme suivante :

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

L'adresse de périphérique locale *baddr1* ou *baddr2*doit figurer à la place de `00:12:34:56:89:90`. Il faut à présent associer à cette interface une adresse IP et l'activer. Utilisez pour ce faire, sur *O1*, les deux commandes :

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

ou, de la même manière, sur *O2* :

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

O1 peut ainsi être joint par *O2* sous l'adresse IP `192.168.1.3`. Avec la commande `ssh 192.168.1.4`, vous pouvez à présent vous connecter sur *O2* à partir d'*O1*, dans la mesure où sshd fonctionne sur *O2* comme c'est le cas par défaut sous SUSE LINUX. La commande `ssh 192.168.1.4` fonctionne du reste désormais aussi en tant qu'utilisateur normal.

Transfert de données d'un téléphone mobile vers l'ordinateur

Le deuxième exemple consiste à transférer sur un ordinateur une image prise par un téléphone portable doté d'un appareil photo (sans coûts supplémentaires liés à l'envoi d'un message multimédia). Notez que chaque téléphone portable possède une arborescence de menus qui lui est propre mais que le processus est la plupart du temps analogue. Consultez si nécessaire le mode d'emploi de votre téléphone. Vous trouverez ci-après une description du transfert d'une photo d'un téléphone Sony Ericsson vers un ordinateur portable. Il faut, pour ce faire, que le service Obex-Push soit disponible sur l'ordinateur et d'autre part que l'ordinateur autorise l'accès au téléphone portable. La première étape consiste à rendre disponible le service sur l'ordinateur portable. Utilisez pour cela le démon opd extrait du paquetage `bluez-utils`. Démarrez-le avec :

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

Deux paramètres sont utilisés : `--sdp` déclare le service auprès de sdpd et `--path /tmp` indique au programme où il doit enregistrer les données reçues— dans le cas présent, dans `/tmp`. Vous pouvez indiquer d'autres chemins exactement de la même manière. Il vous suffit de disposer des droits d'écriture dans le répertoire concerné.

À présent, le téléphone portable doit reconnaître l'ordinateur. Cherchez alors le menu 'Connexions' du téléphone et choisissez l'option 'Bluetooth'. Allez dans 'Se connecter' avant de choisir l'option 'Propre appareil'. Choisissez 'Nouvel appareil' et laissez votre téléphone chercher l'ordinateur portable. Lorsqu'un appareil est trouvé, son nom s'affiche à l'écran. Choisissez l'appareil correspondant à l'ordinateur portable. Une demande de numéro d'identification personnel doit ensuite s'afficher, dans laquelle vous devez saisir le numéro d'identification personnel extrait de `/etc/bluetooth/pin`. Cela permet ainsi au téléphone de reconnaître le portable et donc d'échanger des données avec celui-ci. Quittez à présent

ce menu et cherchez le menu des photos. Choisissez une photo que vous souhaitez transférer, puis appuyez sur le bouton 'Plus'. Dans le menu qui s'affiche à présent, 'Envoyer', vous disposez d'un choix de différents modes d'expédition. Choisissez 'Par Bluetooth'. Le portable doit à présent pouvoir être choisi comme appareil cible. Une fois l'ordinateur sélectionné, le transfert a lieu et la photo est placée dans le répertoire indiqué par la commande `opd`. Vous pourriez procéder de la même manière bien entendu pour transférer un morceau de musique.

17.2.6 Problèmes possibles et solutions

En cas de problème de connexion, veuillez vérifier les points de la liste suivante. N'oubliez cependant pas que le problème peut se trouver de part et d'autre de la connexion, et dans le pire des cas des deux côtés. Dans la mesure du possible, vous devez essayer de comprendre le problème en utilisant un appareil Bluetooth supplémentaire afin de pouvoir écarter les problèmes liés au matériel.

L'appareil local apparait-il dans le résultat de la commande `hcitool dev` ?
Si le périphérique local n'est pas affiché, c'est que soit hcid n'est pas démarré, soit que l'appareil n'est pas reconnu en tant qu'appareil Bluetooth (soit parce que le pilote ne le reconnaît pas, soit parce que l'appareil est défectueux). Les ordinateurs portables avec Bluetooth intégré sont souvent équipés d'un interrupteur pour des périphériques sans fil tels que WLAN et Bluetooth. Vérifiez le manuel de votre ordinateur portable pour voir si votre appareil a un tel interrupteur. Utilisez la commande `rcbluetooth restart` pour redémarrer le démon et consultez `/var/log/messages` pour rechercher d'éventuelles erreurs.

Votre adaptateur Bluetooth nécessite-t-il un microprogramme (firmware) ?
Dans ce cas, veuillez installer `bluez-bluefw` et redémarrer le système Bluetooth avec la commande `rcbluetooth restart`.

La commande `hcitool inq` renvoie-t-elle d'autres appareils ?
Testez cette commande plusieurs fois. Il peut arriver que la connexion ait des interférences parce que la bande de fréquence utilisée par Bluetooth est également utilisée par d'autres appareils.

Les numéros d'identification personnels sont-ils corrects ?
Vérifiez si le numéro d'identification personnel (dans `/etc/bluetooth/pin`) correspond à celui de l'appareil cible utilisé.

L'appareil distant "voit-il" votre ordinateur ?
Essayez d'établir la connexion à partir de l'autre périphérique. Vérifiez si cet appareil voit l'ordinateur.

Est-il possible de construire une connexion réseau (voir exemple 1) ?
Si le premier exemple (connexion réseau) ne fonctionne pas, il existe plusieurs causes possibles : tout d'abord, cela peut être dû au fait que l'un des deux ordinateurs ne comprend pas le protocole ssh. Essayez de voir si `ping 192.168.1.3` ou `ping 192.168.1.4` fonctionnent. Dans l'affirmative, vérifiez si sshd fonctionne. Un autre problème peut être que l'un des deux périphériques a des paramètres qui entrent en conflit avec l'adresse `192.168.1.X` citée dans l'exemple. Essayez tout simplement avec d'autres adresses, telles que `10.123.1.2` et `10.123.1.3`.

L'ordinateur portable apparait-il comme appareil cible (exemple 2) ? L'appareil mobile reconnaît-il le service Obex-Push sur l'ordinateur portable ?
Allez dans le menu 'Appareil propre' de l'appareil concerné et affichez la 'Liste des services'. Si Obex-Push n'y figure pas (même après la mise à jour de la liste), le problème vient alors d'opd sur le portable. opd est-il démarré ? Disposez-vous des droits d'écriture dans le répertoire indiqué ?

Le second exemple fonctionne-t'il en sens inverse ?
Si vous avez installé le paquetage `obexftp`, la commande `obexftp -b ⟨adresseappareil⟩ -B 10 -p image` peut être utilisé pour quelques appareils. Différents modèles des marques Siemens et Sony Ericsson ont été testés et fonctionnent. Veuillez pour cela consulter la documentation du paquetage `/usr/share/doc/packages/obexftp`.

17.2.7 Informations complémentaires

Vous trouverez une bonne vue d'ensemble des différentes procédures à suivre pour utiliser et configurer Bluetooth à l'adresse suivante : `http://www.holtmann.org/linux/bluetooth/` Autres informations et instructions utiles :

- Howto officiel pour la *pile de protocoles Bluetooth* intégrée au noyau (page en anglais) : `http://bluez.sourceforge.net/howto/index.html`
- Connexion avec un assistant numérique personnel PalmOS (page en anglais) : `http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html`

17.3 Transmission de données par infrarouge

IrDA (en anglais, Infrared Data Association) est un standard de communication sans fil par infrarouge. De nombreux ordinateurs portables commercialisés actuellement sont équipés d'un émetteur/récepteur compatible irDA qui permet la communication avec d'autres appareils, tels que les imprimantes, les modems, les réseaux locaux ou d'autres ordinateurs portables. Le débit varie de 2 400 bps jusqu'à 4 Mbps.

Il existe deux modes d'exploitation pour IrDA. En mode par défaut SIR, on communique avec le port infrarouge au moyen d'une interface série. Ce mode fonctionne sur presque tous les appareils et est suffisant dans de nombreux cas. Le mode le plus rapide FIR nécessite un pilote spécial pour le composant IrDA. Il n'existe cependant pas de tel pilote pour tous les composants. De plus, il faut régler le mode souhaité lors de la configuration du BIOS de l'ordinateur. C'est également là que vous voyez quelle interface série est utilisée pour le mode SIR.

Vous trouverez des informations au sujet de l'IrDA dans le howto de Werner Heuser sous `http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html` et sur le site Web du projet IrDA Linux : `http://irda.sourceforge.net/`.

17.3.1 Logiciels

Vous trouverez les modules de noyau nécessaires dans le paquetage du noyau. Le paquetage `irda` prépare les utilitaires pour la prise en charge de l'interface infrarouge. Une fois le paquetage installé, vous trouverez la documentation correspondante à l'emplacement `/usr/share/doc/packages/irda/README`.

17.3.2 Configuration

Le service système IrDA n'est pas automatiquement démarré lors de l'amorçage. Utilisez le module IrDA de YaST pour son activation. Seul un paramètre y est modifiable : l'interface série du périphérique infrarouge. Dans la fenêtre de test proposée, il existe deux sorties. La première est celle de `irdadump` qui journalise tous les paquets IrDA émis et reçus. Dans cette sortie, le nom de l'ordinateur et les noms de tous les appareils infrarouges à portée devraient apparaître régulièrement. Vous trouvez un exemple de cette sortie dans section 17.3.4 page 371. Tous

les appareils avec lesquels il existe une liaison IrDA apparaissent dans la partie inférieure de la fenêtre.

Malheureusement, l'IrDA nécessite beaucoup plus d'énergie (de la batterie) car toutes les deux secondes un paquetage de découverte est envoyé pour la reconnaissance d'autres périphériques. C'est pour cette raison qu'il est conseillé, lorsque vous souhaitez économiser vos batteries, de ne démarrer l'IrDA qu'à la demande. Utilisez la commande `rcirda start` pour activer manuellement l'interface à tout instant ou `rcirda stop` pour la désactiver. Lorsque l'interface est activée, les modules du noyau nécessaires sont automatiquement chargés.

Vous pouvez procéder à la configuration manuelle dans le fichier `/etc/sysconfig/irda`. Celui-ci ne contient qu'une variable, `IRDA_PORT`, qui définit quelle interface utiliser en mode SIR.

17.3.3 Utilisation

Si vous souhaitez imprimer des documents par infrarouge, vous pouvez envoyer vos données via le fichier de périphériques `/dev/irlpt0`. Le fichier de périphériques `/dev/irlpt0` se comporte comme l'interface connectée par un câble normal `/dev/lp0`, à la différence que les données à imprimer sont transmises sans fil par de la lumière infrarouge. Lors de l'impression, veillez à ce que l'imprimante soit à portée de l'interface infrarouge de l'ordinateur et que la prise en charge de l'infrarouge soit démarrée.

Vous pouvez configurer une imprimante exploitée par l'intermédiaire d'une interface infrarouge comme à votre habitude, à l'aide de YaST. L'imprimante n'est pas reconnue automatiquement, configurez-la alors manuellement en cliquant sur 'Autres (pas reconnues)'. Dans le dialogue suivant, vous pouvez sélectionner 'Imprimante via IrDA'. Comme port `irlpt0` est pratiquement toujours correct. Vous trouverez des détails sur l'utilisation des imprimantes sous Linux dans chapitre 12 page 261.

Si vous souhaitez utiliser l'interface infrarouge avec d'autres ordinateurs, des téléphones portables ou d'autres appareils de ce type, vous pouvez le faire au moyen du fichier de périphériques `/dev/ircomm0`. Ainsi avec les téléphones portables S25 de Siemens et 6210 de Nokia, vous pouvez vous connecter à l'Internet sans fil par de l'infrarouge grâce au programme wvdial. Une synchronisation des données avec un Palm Pilot est également possible, il vous suffit de saisir simplement le nom de périphérique `/dev/ircomm0` dans le programme correspondant.

Vous ne pouvez communiquer qu'avec les appareils qui prennent en charge les protocoles Printer ou IrCOMM. Vous pouvez utiliser des programmes spéciaux comme irobexpalm3 ou irobexreceive pour vous adresser à des appareils comme le 3Com Palm Pilot qui utilisent le protocole IROBEX. Vous trouverez plus d'informations à ce sujet dans *IR-HOWTO* (`http://tldp.org/HOWTO/Infrared-HOWTO/`). La liste des protocoles pris en charge par l'appareil est affichée par `irdadump` après le nom de l'appareil entre crochets. La prise en charge du protocole IrLAN est toujours "en cours de développement".

17.3.4 Problèmes possibles et solutions

Si certains appareils ne réagissent pas au niveau du port infrarouge, vous pouvez, en tant qu'utilisateur `root`, saisir la commande `irdadump` pour vérifier si l'autre appareil est reconnu par l'ordinateur.

Dans le cas d'une imprimante BJC-80 Canon en vue de l'ordinateur, on obtient alors un résultat semblable au suivant et qui se répète régulièrement (voir le résultat exemple 17.1 de la présente page).

Example 17.1: *Sortie d'irdadump*

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* terre
                        hint=0500 [ PnP Computer ] (21)
```

Si aucun résultat n'est obtenu ou si l'autre appareil ne se signale pas en retour, vérifiez la configuration de l'interface. Utilisez-vous vraiment la bonne interface ? Vous trouverez parfois aussi l'interface infrarouge sous le nom `/dev/ttyS2` ou `/dev/ttyS3` ou un autre quand l'interruption 3 est utilisée. Vous pouvez toutefois configurer ces paramètres pour presque tous les ordinateurs portables dans la configuration du BIOS.

Vous pouvez aussi utiliser une caméra vidéo pour facilement vérifier si la LED infrarouge s'allume. Contrairement aux yeux de l'homme, la plupart des caméras vidéos peuvent voir la lumière infrarouge.

Le système Hotplug

Le système de branchement à chaud (hotplug) contrôle l'initialisation de la plupart des périphériques dans un ordinateur. Il n'est pas seulement utilisé pour les périphériques pouvant être insérés et retirés durant le fonctionnement mais pour tous les périphériques qui sont reconnus durant l'amorçage du noyau. Il travaille en étroite collaboration avec le système de fichiers `sysfs` et `udev` qui sont décrits dans le chapitre 19 page 383.

Jusqu'à ce que le noyau soit amorcé, seuls les périphériques absolument nécessaires, comme le système de bus, les disques d'amorçage et le clavier, sont initialisés. Normalement, le noyau déclenche un événement hotplug pour tous les périphériques détectés. Le démon `udevd` écoute ces événements et appelle les scripts hotplug correspondants afin d'initialiser ces périphériques. Pour les périphériques qui ne sont pas reconnus automatiquement ou dont les événements ont été perdus lors de l'amorçage, vous disposez de coldplug. Il repasse le événements enregistrés ou balaie le système à la recherche de périphériques non initialisés et utilise une configuration statique aux anciens périphériques tels que ISA.

Si on laisse de côté quelques exceptions historiques, la plupart des périphériques sont initialisés dès qu'ils sont disponibles, soit à l'amorçage du système ou au branchement. Durant cette initialisation, les interfaces sont enregistrées par le noyau. L'enregistrement de l'interface entraîne d'autres événements hotplug qui déclenchent une installation automatique de l'interface concernée.

Dans les versions précédentes de SUSE LINUX, un ensemble statique de données de configuration était utilisé pour initialiser les périphériques. Maintenant le système examine chaque périphérique disponible et recherche les données de configuration adéquates ou le génère.

Les plus importantes fonctions hotplug sont configurées dans deux fichiers : vous trouverez dans `/etc/sysconfig/hotplug` des variables qui commandent le comportement de `hotplug` et `coldplug`. Chaque variable est détaillée par un commentaire. Le fichier `/proc/sys/kernel/hotplug` comporte le nom du programme exécutable qui est appelé par le noyau. Les réglages de périphériques se trouvent dans le fichier `/etc/sysconfig/hardware`. À partir de SUSE LINUX 9.3, ce fichier est normalement vide car `udevd` reçoit les messages hotplug via un socket netlink.

18.1 Périphériques et interfaces

Le système hotplug ne gère pas que des interfaces mais aussi des périphériques. Un périphérique est lié soit à un bus, soit à une interface. Un bus peut être considéré comme une interface multiple. Une interface relie des périphériques entre eux ou à une application. Il existe aussi des périphériques virtuels tels que des tunnels réseau. Les périphériques nécessitent généralement des pilotes sous forme de modules du noyau. Les interfaces sont principalement représentées par des nœuds de périphériques créés par `udev`. La distinction entre périphériques et interfaces est importante pour la compréhension du concept général.

On trouve dans /sys/devices les périphériques déclarés dans le système de fichiers sysfs ; les interfaces se trouvent dans /sys/class ou /sys/block. Dans le fichier sysfs, toutes les interfaces doivent comporter un lien (*en anglais link*) vers leur périphérique. Toutefois, il existe encore quelques pilotes qui n'ajoutent pas automatiquement ce lien. Sans ce lien, on ne sait pas à quel périphérique appartient cette interface et il est impossible de trouver une configuration adaptée.

Les périphériques sont identifiés au moyen d'une description de périphérique. Celle-ci peut être le chemin de périphérique (device path) dans sysfs (/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0), une description de l'emplacement de connexion (bus-pci-0000:02:00.0), un identifiant individuel (id-32311AE03FB82538) ou toute méthode comparable d'identification. Auparavant les interfaces étaient toujours identifiées par leur nom. Ces noms sont une simple numérotation des périphériques existants, qui peuvent donc avoit été modifiés lorsque les périphériques ont été ajoutés ou supprimés.

On peut aussi identifier les interfaces par une description du périphérique correspondant. C'est alors généralement le contexte qui permet de déterminer si c'est de la description du périphérique lui même ou de son interface dont il est question. Des exemples typiques de périphériques, d'interfaces et de leurs descriptions sont :

Carte réseau PCI Un périphérique lié au bus PCI (/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0 ou bus-pci-0000:02:00.0) et qui dispose d'une interface réseau (eth0, id-00:0d:60:7f:0b:22 ou bus-pci-0000:02:00.0). Celle-ci est utilisée par des services réseau ou est liée à un périphérique réseau virtuel comme un tunnel ou un réseau local virtuel (VLAN), lequel possède en retour une interface.

Contrôleur PCI SCSI Un périphérique (/sys/devices/pci0000:20/0000:20:01.1, etc.) qui met à disposition plusieurs interfaces physiques sous la forme d'un bus (/sys/class/scsi_host/host1).

Disque dur SCSI Un périphérique (/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0, bus-scsi-1:0:0:0) avec plusieurs interfaces (/sys/block/sda*).

18.2 Événements hotplug

Chaque périphérique et chaque interface a un *événement hotplug* associé qui est traité par udev et l'agent hotplug correspondant. Les événements hotplug sont

déclenchés par le noyau lorsqu'un lien vers un périphérique est établi ou supprimé ou lorsqu'un pilote enregistre ou efface une interface. Depuis SUSE LINUX 9.3, `udevd` reçoit et distribue des événements hotplug. Soit `udevd` écoute directement les messages netlink depuis le noyau, soit `/sbin/udevsend` doit être spécifié dans `/proc/sys/kernel/hotplug`. Une fois que `udevd` a fait sont travail (voir le chapitre 19 page 383), il recherche, dans `/etc/hotplug.d/`, un agent hotplug qui correspond au type de l'événement.

18.3 Agents hotplug

Un agent hotplug est un programme exécutable qui accomplit les actions appropriées pour un événement. Pour les événements de périphériques, les agents se trouvent dans `/etc/hotplug.d/`⟨*nom événement*⟩ et

`/etc/hotplug.d/default`. Dans ces répertoires, tous les programmes qui ont le suffixe `.hotplug` sont exécutés par ordre alphabétique.

Pour s'assurer que les événement d'un genre particulier sont ignorés, supprimez les bits exécutables des agents hotplug respectifs. Vous pouvez aussi changer le suffixe `.hotplug` en quelque chose d'autre.

Les agents de périphériques chargent en majorité des modules de noyau, mais doivent occasionnellement appeler aussi des commandes supplémentaires. Sous SUSE LINUX, ceci est pris en charge par `/sbin/hwup` ou `/sbin/hwdown`. Ces programmes recherchent dans le répertoire `/etc/sysconfig/hardware` une configuration adaptée au périphérique et l'utilisent. Si un périphérique donné ne doit pas être initialisé, un fichier de configuration correspondant doit être mis en place avec le mode de démarrage `manual` ou `off`. Si `/sbin/hwup` ne trouve aucune configuration, les modules sont automatiquement chargés par l'agent. Dans ce cas, certains agents génèrent automatiquement des fichiers de configuration pour `hwup`. Cela rendra l'agent plus rapide la prochaine fois. Pour plus d'informations sur ce sujet, voir la section 18.4 page 378. Vous trouverez des informations sur `/sbin/hwup` dans le fichier `/usr/share/doc/packages/sysconfig/README` et dans la page de manuel `man hwup`.

Avant que les agents d'interfaces soient appelés, `udev` construit d'abord un nœud de périphérique (en anglais device node) auquel le système a accès. `udev` permet de donner des noms persistants aux interfaces. Voir le chapitre 19 page 383 pour plus de détails. Enfin, les agents individuels installent les interfaces. Les opérations correspondant à quelques interfaces sont décrites dans ce qui suit.

18.3.1 Activation des interfaces réseau

Les interfaces réseau sont initialisées avec /sbin/ifup et désactivées avec /sbin/ifdown. Vous trouverez des détails à ce sujet dans le fichier /usr/share/doc/packages/sysconfig/README et dans la page de manuel man ifup.

Si un ordinateur dispose de plusieurs périphériques réseau avec différents pilotes, il se peut que les désignations d'interfaces soient modifiées si un autre pilote a été chargé plus rapidement lors de l'amorçage. C'est pour cela que dans SUSE LINUX les événements des périphériques réseau PCI sont administrés par une file d'attente. Vous pouvez désactiver ce comportement dans le fichier /etc/sysconfig/hotplug par l'intermédiaire de la variable HOTPLUG_PCI_QUEUE_NIC_EVENTS=no.

Cependant, la meilleure solution est d'utiliser des désignations d'interfaces cohérentes. Vous pouvez spécifier le nom souhaité dans les fichiers de configuration de chaque interface. Vous trouverez des détails sur cette méthode dans le fichier /usr/share/doc/packages/sysconfig/README. Depuis SUSE LINUX 9.3, udev se charge aussi des interfaces réseau bien qu'ils ne s'agissent pas de nœuds de périphérique. Ceci permet l'utilisation de noms d'interface persistants de façon plus standardisée.

18.3.2 Activation des périphériques de stockage

Les interfaces des périphériques de stockage doivent être montées pour pouvoir y accéder. Cela peut soit se faire de façon totalement automatique, soit être configuré à l'avance. La configuration s'effectue dans le fichier /etc/sysconfig/hotplug au moyen des variables HOTPLUG_DO_MOUNT, HOTPLUG_MOUNT_TYPE et HOTPLUG_MOUNT_SYNC et dans le fichier /etc/fstab. Le fonctionnement complètement automatisé est activé en fixant la variable HOTPLUG_DO_MOUNT=yes. Désactivez-le en attribuant la valeur no à la variable.

Utilisez la variable HOTPLUG_MOUNT_TYPE pour basculer entre deux modes : subfs ou fstab. En mode HOTPLUG_MOUNT_TYPE=subfs, un sous-répertoire dont le nom est construit à partir des caractéristiques du périphérique est placé dans le répertoire /media. Le volume y est monté et démonté automatiquement par la commande submountd lorsque l'on accède au support. Les périphériques utilisant ce mode peuvent facilement être retirés lorsque l'on y accède plus. En mode HOTPLUG_MOUNT_TYPE=fstab, les périphériques de stockage sont montés de manière traditionnelle comme il est indiqué dans le fichier /etc/fstab.

La variable HOTPLUG_MOUNT_SYNC permet de choisir si l'accès doit se faire en mode synchrone ou asynchrone. En fonctionnement asynchrone, le temps d'accès en écriture est plus court, car les résultats sont stockés dans un tampon. Il se peut toutefois que les données ne puissent pas être écrites complètement lorsque le support est retiré sans précaution. En fonctionnement synchrone, toutes les données sont écrites immédiatement, mais le temps d'accès est plus long. Il faut démonter le périphérique manuellement avec la commande umount.

L'utilisation de noms persistants pour les périphériques est recommandées car les noms de périphériques traditionnels peuvent changer selon l'ordre d'initialisation. Vous pourrez trouver plus de détails sur les noms persistants pour les périphériques dans le chapitre 19 page 383.

18.4 Chargement automatique de modules

Si un périphérique ne peut pas être initialisé avec /sbin/hwup, l'agent explore les *tables de correspondance de modules* (en anglais module maps) à la recherche d'un pilote adapté. Il examine en premier les tables de correspondance dans /etc/hotplug/*.handmap ; s'il n'a pas trouvé de pilote, il cherche également dans /lib/modules/<kernelversion>/modules.*map. Si vous voulez utiliser un autre pilote que le pilote standard du noyau, déclarez-le dans /etc/hotplug/*.handmap car ce fichier est le premier à être lu.

L'agent USB cherche également des pilotes en mode utilisateur dans les fichiers /etc/hotplug/usb.usermap et /etc/hotplug/usb/*.usermap. Les pilotes en mode utilisateur (user-mode) sont des programmes qui règlent l'accès au périphérique en lieu et place d'un module noyau. On peut de cette façon appeler des programmes exécutables pour des périphériques déterminés.

Dans le cas de périphériques PCI, pci.agent interroge d'abord hwinfo au sujet de modules de pilote. L'agent ne recherche dans le pci.handmap et les correspondances du noyau (kernel map) que si hwinfo ne connaît aucun pilote. Ceci a déjà été tenté auparavant par hwinfo et doit donc également échouer. hwinfo dispose d'une base de données supplémentaire d'assignation des pilotes. Toutefois la commande lit également pci.handmap, ce qui permet de s'assurer qu'une quelconque assignation inscrite dans ce fichier est réellement utilisée.

L'agent pci.agent peut être limité à des périphériques d'un type déterminé ou aux modules pilotes qui se trouvent dans un sous-répertoire de /lib/modules/<kernelversion>/kernel/drivers. Dans le premier cas, des classes de périphériques PCI trouvées à la fin du fichier /usr/share/pci.ids peuvent être

ajoutées dans le fichier /etc/sysconfig/hotplug au niveau des variables HOTPLUG_PCI_CLASSES_WHITELIST etHOTPLUG_PCI_CLASSES_BLACKLIST. Pour le second cas, spécifiez un ou plusieurs répertoires dans les variables HOTPLUG_PCI_DRIVERTYPE_WHITELIST et HOTPLUG_PCI_DRIVERTYPE_-BLACKLIST. Les modules de ces répertoires exclus ne sont jamais chargés. Dans les deux cas, une liste blanche (whitelist) totalement vide signifie que toute possibilité, à l'exception de celles exclues dans la liste noire (blacklist), est autorisée. Vous pouvez également exclure des modules individuels du chargement. Indiquez simplement dans le fichier /etc/hotplug/blacklist les modules qui ne devront jamais être chargés par un agent. Écrivez chacun des noms de module sur une ligne séparée.

Si plusieurs modules appropriés sont trouvés dans une table de correspondance, seul le premier module sera chargé. Si vous souhaitez que tous les modules soient chargés, déclarez la variable HOTPLUG_LOAD_MULTIPLE_-MODULES=yes. Il est préférable toutefois d'établir une configuration matérielle /etc/sysconfig/hardware/hwcfg-* particulière pour ce périphérique.

Cela ne concerne pas les modules chargés à l'aide de hwup. Le chargement automatique de modules n'a lieu qu'exceptionnellement, et sera encore davantage restreint dans les versions futures de SUSE LINUX. Cependant, si un module adéquat a été trouvé, l'agent crée un fichier de configuration hwup qui sera utilisé la prochaine fois. Cela augmente la vitesse d'initialisation du périphérique.

18.5 Hotplug avec PCI

Quelques ordinateurs autorisent également le branchement à chaud de périphériques PCI. Afin de pouvoir utiliser pleinement cette possibilité, des modules de noyau particuliers doivent être chargés. Ces modules peuvent toutefois créer des problèmes sur les ordinateurs ne disposant pas de PCI hotplug. Les emplacements PCI hotplug ne peuvent malheureusement pas être reconnus automatiquemen. Pour configurer cette fonction manuellement, attribuez la valeur yes à la variable HOTPLUG_DO_REAL_PCI_HOTPLUG dans le fichier /etc/sysconfig/hotplug.

18.6 Le script d'amorçage Coldplug

La commande boot.coldplug est utilisée pour tous les périphériques qui ne sont pas reconnus automatiquement, c'est-à-dire pour lesquels aucun événement

hotplug n'a pu être généré. C'est simplement la commande hwup qui est appelée pour chaque configuration matérielle statique nommée /etc/sysconfig/hardware/hwcfg-static-*. Ceci peut également être utilisé pour initialiser des périphériques intégrés dans un ordre différent de celui qui serait utilisé par hotplug : en effet, la commande coldplug est exécutée avant hotplug.

18.7 Analyse d'erreurs

18.7.1 Fichiers journaux

hotplug n'envoie en standard que quelques informations importantes à syslog. Pour recevoir plus d'informations, configurez la variable HOTPLUG_-DEBUG du fichier /etc/sysconfig/hotplug à la valeur yes. Si vous donnez à cette variable la valeur max, chaque commande de l'interpréteur de commandes de tous les scripts hotplug sera consignée. Ceci signifie que la taille du fichier /var/log/messages dans lequel syslog enregistre tous les messages sera beaucoup plus importante. Comme, lors de l'amorçage, syslog n'est démarré qu'après hotplug et coldplug, il est possible que les premières informations ne soient pas consignées. Si ces informations sont importantes pour vous, créez au moyen de la variable HOTPLUG_SYSLOG un autre fichier de journal. Des informations sur ce sujet sont disponibles dans /etc/sysconfig/hotplug.

18.7.2 Problèmes d'amorçage

Si un ordinateur se fige au cours du processus d'amorçage, désactivez hotplug ou coldplug en entrant NOHOTPLUG=yes ou NOCOLDPLUG=yesdans l'invite d'amorçage. La désactivation de hotplug a pour conséquence qu'aucun événement hotplug n'est émis par le noyau. Vous pouvez réactiver hotplug pendant que le système est en marche en entrant la commande /etc/init.d/boot.hotplug start. Tous les événements hotplug créés jusqu'à ce moment sont alors émis et traités. Pour supprimer des événements de la file d'attente, indiquez auparavant /bin/true dans /proc/sys/kernel/hotplug, puis, après un certain temps, revenez à la valeur /sbin/hotplug. La désactivation de coldplug a pour conséquence que les réglages statiques ne sont pas appliqués. Vous pouvez appliquer ultérieurement la configuration statique en entrant la commande /etc/init.d/boot.coldplug start.

Pour savoir si un module donné, chargé par hotplug, est responsable des problèmes, tapez HOTPLUG_TRACE=<N> dans l'invite d'amorçage. Les noms de tous

les modules à charger sont alors affichés l'un après l'autre à l'écran avant d'être effectivement chargés après ⟨N⟩ secondes. Vous ne pouvez cependant pas intervenir ici de façon interactive.

18.7.3 L'enregistreur d'événements

Le script `/sbin/hotplugeventrecorder` est appelé à chaque événement par `/sbin/hotplug`. S'il existe un répertoire `/events`, tous les événements hotplug y sont enregistrés comme des fichiers individuels. De cette façon, on peut générer à nouveau des événements à des fins de test. Si le répertoire n'existe pas, aucun enregistrement n'est créé.

Nœuds de périphériques dynamiques avec udev

Avec le noyau Linux 2.6, il existe une nouvelle solution *user space* pour un répertoire de périphériques `/dev` dynamique avec des désignations de périphériques persistantes : `udev`. Cette solution fournit les fichiers uniquement pour les périphériques réellement présents. Elle crée ou supprime les fichiers nœuds des périphériques distants situés généralement dans le répertoire `/dev` et elle renomme les interfaces réseau. L'implémentation précédente de `/dev` avec `devfs` ne fonctionne plus et est remplacée par `udev`.

Des nœuds de périphériques (*en anglais, device nodes*) ont été traditionnellement enregistrés sur les systèmes Linux dans le répertoire `/dev`. Il existait un nœud pour chaque type de périphérique, indépendamment du fait de savoir s'il existait effectivement dans le système. En conséquence, la taille de ce répertoire devenait importante. On a connu une amélioration sensible avec `devfs` car seuls les périphériques existant réellement obtenaient un nœud de périphériques dans `/dev`.

`udev` s'y prend autrement pour créer des nœuds de périphériques. Il compare les informations mises à disposition par `sysfs` avec les entrées fournies par l'utilisateur sous forme de règles. `sysfs` est un nouveau système de fichiers du noyau 2.6. Il donne les informations de base sur les périphériques connectés dans le système. Il est monté sous `/sys`.

L'utilisateur ne doit pas absolument créer de règles. Si on connecte un périphérique, le nœud de périphérique correspondant est alors créé. Les règles offrent cependant la possibilité de modifier le nom des nœuds. Ceci permet de remplacer le nom cryptique d'un périphérique par un nom de périphérique plus facile à retenir, et de conserver en outre des noms de périphériques persistants si vous avez connecté deux périphériques de même type.

Par défaut, deux imprimantes reçoivent les désignations `/dev/lp0` et `/dev/lp1`. Quel nœud de périphérique est attribué à chacune dépend de l'ordre dans lequel elles ont été mises sous tension. Un autre exemple sont les périphériques de mémoire de masse comme les disques durs USB. Avec la commande `udev`, on entre les chemins exacts du périphérique dans `/etc/fstab`.

19.1 Création de règles

Avant que `udev` crée des nœuds de périphériques sous `/dev`, il lit, par odre alphabétique, tous les fichiers de `/etc/udev/rules.d` qui ont le suffixe `.rules`. La première règle qui convient à un périphérique est utilisée, même s'il en existe d'autres. Les commentaires commencent par le signe #. Les règles ont la forme suivante :

```
Code, [Code,...] NOM [, SYMLINK]
```

Un code au minimum doit être indiqué car la règle va être affectée à un périphérique par l'intermédiaire de ce code. Il est également nécessaire de spécifier le nom. Le nœud de périphérique sera établi sous ce nom dans `/dev`. Le paramètre symlink optionnel permet d'établir des nœuds de périphériques dans d'autres endroits. Une règle pour une imprimante pourrait avoir la forme suivante :

```
BUS="usb", SYSFS{serial}="12345", NAME="lp_hp", SYMLINK="printers/hp"
```

Il y a dans cet exemple deux codes : `BUS` et `SYSFS{serial}`. `udev` compare le numéro de série avec celui du périphérique auquel le bus USB est connecté. Tous les codes doivent être identiques afin d'attribuer au périphérique le nom `lp_hp` dans le répertoire `/dev`. De plus, un lien symbolique `/dev/printers/hp` qui renvoie au nœud de périphérique est créé. Dans le même temps, le répertoire `printers` est créé automatiquement. Les requêtes d'impression peuvent ensuite être envoyées à `/dev/printers/hp` ou `/dev/lp_hp`.

19.2 Automatisation avec NAME et SYMLINK

Les paramètres NAME et SYMLINK permettent l'utilisation d'opérateurs pour l'automatisation des affectations. Ces opérateurs se réfèrent à des données du noyau au sujet du périphérique correspondant. Voici un exemple simple en guise d'illustration :

```
BUS="usb", SYSFS{vendor}="abc", SYSFS{model}="xyz", NAME="camera%n"
```

L'opérateur %n est remplacé dans le nom par le numéro prévu pour l'appareil photo périphérique : `camera0` ou `camera1`. Un autre opérateur utile est `%k`, remplacé par le nom du périphérique standard du noyau, par exemple `hda1`. Vous pouvez également faire appel à un programme externe dans les règles udev et utiliser la chaîne qui est donnée dans les valeurs NAME et SYMLINK. La page de manuel de `udev` vous donne une liste de tous les opérateurs.

19.3 Expressions régulières dans les codes

Dans les codes des règles udev, vous pouvez utiliser des caractères de remplacement de style shell appelés jokers. Ainsi, par exemple, le signe `*` qui peut être utilisé en tant que caractère de remplacement pour n'importe quel chaîne de caractères ou `?` qui peut être utilisé comme caractère de remplacement pour exactement un caractère arbitraire.

```
KERNEL="ts*", NAME="input/%k"
```

Avec cette règle, un périphérique, dont la désignation commence avec les lettres "ts", reçoit le nom de noyau standard dans le répertoire standard. Vous trouverez des informations détaillées sur l'utilisation d'expressions régulières dans les règles udev à la page de manuel `man udev`.

19.4 Sélection de codes

Le choix d'un bon code est essentiel pour toute règle udev apte à fonctionner. Les codes standard sont par exemple :

BUS type de bus du périphérique

NOYAU nom du périphérique que le noyau utilise

ID numéro du périphérique sur le bus (par exemple, Bus PCI ID)

PLACE emplacement physique auquel le périphérique est connecté (par exemple, sur USB)

SYSFS{...} attributs de périphérique sysfs tels que étiquette, constructeur, numéro de série, etc.

Les codes `ID` et `PLACE` peuvent s'avérer utiles, mais la plupart du temps les codes `BUS` et `KERNEL` ainsi que `SYSFS{...}` sont utilisés. De plus, la configuration de `udev` met à disposition des codes qui appellent des scripts externes et évaluent leur résultat. Vous trouverez plus de détails à ce sujet dans la page de manuel `man udev`.

Le système de fichiers `sysfs` enregistre des petits fichies contenant des informations matérielles dans une arborescence de répertoire. En règle générale, chaque fichier ne contient qu'une information, comme le nom du périphérique, le fabricant et le numéro de série. Chacun de ces fichiers peut être utilisé comme valeur de code. Si vous voulez utiliser plusieurs codes SYSFS dans une règle, vous ne devez cependant utiliser que des fichiers du même répertoire comme valeurs de code. L'outil `udevinfo` peut être utile pour trouver des valeurs de code.

Vous devez trouver un sous-répertoire de `/sys` qui se rapporte au périphérique correspondant et contient un fichier `dev`. Vous trouverez tous ces répertoires sous `/sys/block` ou `/sys/class`. S'il existe déjà un nœud de périphérique pour le périphérique, `udevinfo` peut trouver le sous-répertoire correct pour vous. La commande `udevinfo -q path -n /dev/sda` affiche `/block/sda`.

Ceci signifie que le répertoire recherché est `/sys/block/sda`. Appelez ensuite `udevinfo` avec la commande `udevinfo -a -p /sys/block/sda`. Les deux commandes peuvent également être combinées comme dans `udevinfo -a -p ‘udevinfo -q path -n /dev/sda‘`. Un extrait de l'affichage pourrait ressembler à ceci :

```
BUS="scsi"
ID="0:0:0:0"
SYSFS{detach_state}="0"
SYSFS{type}="0"
SYSFS{max_sectors}="240"
SYSFS{device_blocked}="0"
SYSFS{queue_depth}="1"
SYSFS{scsi_level}="3"
SYSFS{vendor}="        "
SYSFS{model}="USB 2.0M DSC    "
SYSFS{rev}="1.00"
SYSFS{online}="1"
```

Sélectionnez dans les sorties d'informations les codes adéquats que vous ne voulez pas modifier. Notez que vous ne pouvez pas utiliser des codes issus de répertoires différents.

19.5 Noms persistants pour périphériques de mémoire de masse

Avec SUSE LINUX sont livrés des scripts qui vous permettent d'affecter les mêmes désignations aux disques durs et autres périphériques de mémoire quelque soit l'ordre dans lequel ils ont été initialisés. `/sbin/udev.get_persistent_device_name.sh` est un script wrapper. Il appelle d'abord `/sbin/udev.get_unique_hardware_path.sh` qui trouve le chemin d'accès vers un périphérique donné. `/sbin/udev.get_unique_drive_id.sh` retrouve le numéro de série. Les deux informations sont transmises à `udev` qui crée des liens symboliques ves le nœud de périphérique sous `/dev`. Le script wrapper peut être utilisé directement dans les règles udev. Voici un exemple pour SCSI, qu'on peut également étendre à USB ou IDE (à saisir sur une seule ligne) :

```
BUS="scsi", PROGRAM="/sbin/udev.get_persistent_device_name.sh",
NAME="%k" SYMLINK="%c{1+}"
```

Dès qu'un pilote pour un périphérique de mémoire de masse a été chargé, il se manifeste auprès du noyau avec tous les disques durs en présence. Chacun d'entre eux déclenchera un événement bloc hotplug qui appelle `udev`. `udev` lit alors les règles afin de constater si un symlink doit être créé.

Si le pilote est chargé via `initrd`, les événements hotplug sont perdus. Cependant, toutes les informations sont enregistrées dans `sysfs`. Le programme d'aide `udevstart` trouve tous les fichiers de périphériques sous `/sys/block` et `/sys/class`, puis démarre `udev`.

Il existe en outre un script de démarrage `boot.udev` qui recrée tous les nœuds de périphériques pendant l'amorçage. Cependant, ce script de démarrage doit être activé via le l'éditeur de niveaux d'exécution de YaST ou à l'aide de la commande `insserv boot.udev`.

Astuce

Il existe un bon nombre d'outils et de programmes qui croient sans réserve que `/dev/sda` est un disque dur SCSI et `/dev/hda` un disque dur IDE. Si cela n'est pas le cas, ces programmes ne fonctionnent plus. Mais YaST dépend de ces outils et ne travaille donc qu'avec les désignations de périphériques du noyau.

Astuce

Systèmes de fichiers sous Linux

Linux prend en charge un certain nombre de systèmes de fichiers différents. Ce chapitre présente un bref tour d'horizon des systèmes de fichiers Linux les plus connus, en insistant sur leur principe de conception, leurs avantages et leurs domaines d'application. Quelques informations complémentaires sur LFS (Large File Support,prise en charge des gros fichiers) sous Linux sont également offertes.

20.1 Terminologie

métadonnées Une structure de données interne à un système de fichiers qui garantit que toutes les données sur le disque sont correctement organisées et accessibles. Il s'agit essentiellement des "données concernant les données". Pratiquement chaque système de fichiers a sa propre structure de métadonnées, ce qui explique en partie la raison pour laquelle les systèmes de fichiers affichent des caractéristiques de performances différentes. Il est particulièrement important de conserver intactes les métadonnées car, sinon, toutes les données présentes sur le système de fichiers pourraient devenir inaccessibles.

inode Les inodes contiennent diverses informations sur un fichier, dont sa taille, le nombre de liens, la date, la date et l'heure de création, les modifications et l'accès ainsi que les pointeurs sur les blocs du disque dans lesquels le contenu des fichiers est effectivement enregistré.

journal Dans le contexte d'un système de fichiers, un journal est une structure sur disque contenant une sorte de fichier journal dans lequel le système de fichiers enregistre ce qui est sur le point de changer dans les métadonnées du système de fichiers. La journalisation réduit considérablement le temps de restauration d'un système Linux, parce qu'il supprime le processus de recherche très long qui vérifie le système de fichiers complet au démarrage du système. À la place, seul le journal est relu.

20.2 Les principaux systèmes de fichiers sous Linux

Contrairement à il y a deux ou trois ans, on ne choisit plus un système de fichiers pour Linux en quelques secondes (Ext2 ou ReiserFS ?). Les noyaux à partir de la version 2.4 proposent une grande variété de systèmes de fichiers. Vous trouverez ci-après une vue d'ensemble des grands principes de fonctionnement de ces systèmes de fichiers et les avantages qu'ils offrent.

Il est très important de considérer qu'il ne peut pas y avoir un système de fichiers qui convienne le mieux à tous les types d'applications. Chaque système de fichiers a ses points forts et ses faiblesses, qu'il faut prendre en compte. Quoi qu'il en soit, même le système de fichiers le plus sophistiqué ne peut pas remplacer une stratégie de sauvegarde raisonnable.

Les termes ”intégrité des données“ et ”cohérence des données“, lorsque utilisés dans ce chapitre, ne font pas référence à la cohérence des données de l'espace utilisateur (les données que votre application écrit sur ses fichiers). C'est l'application elle-même qui doit assurer la cohérence de ces données.

Important

Configurer les systèmes de fichiers

Sauf indication contraire dans ce chapitre, toutes les étapes requises pour configurer ou changer des partitions et des systèmes de fichiers peuvent avoir lieu à l'aide du module de YaST.

Important

20.2.1 ReiserFS

Officiellement, une des fonctionnalités phares de la version 2.4 du noyau, ReiserFS était disponible sous forme de correctif de noyau pour les noyaux SUSE 2.2.x depuis la version 6.4 de SUSE LINUX. ReiserFS a été conçu par Hans Reiser et l'équipe de développement Namesys. ReiserFS a prouvé qu'il était une puissante alternative à l'ancien Ext2. Ses principaux atouts sont : une meilleure gestion de l'espace disque, de meilleures performances d'accès aux disques et une restauration plus rapide après une panne.

Les points forts de ReiserFS, de manière plus détaillée, sont :

Une meilleure gestion de l'espace disque

Dans ReiserFS, toutes les données sont organisées dans une structure dénommée arbre équilibré B^*. Cette structure arborescente contribue à une meilleure gestion de l'espace disque car des petits fichiers peuvent être enregistrés directement dans les feuilles de l'arbre B^* au lieu de l'être à d'autres endroits en se contentent de tenir à jour un pointeur sur l'emplacement réel du disque. En plus de cela, le stockage n'est pas alloué en blocs de 1 ou de 4 ko, mais en portions de la taille exacte nécessaire. Un autre avantage se situe dans l'allocation dynamique des inodes. Ce comportement confère au système de fichiers une plus grande flexibilité par rapport aux systèmes de fichiers classiques, comme Ext2, dans lesquels il faut spécifier la densité d'inodes au moment où l'on crée le système de fichiers.

Meilleures performances d’accès aux disques
Pour de petits fichiers, les données des fichiers et les informations (inodes) ”stat_data“ sont souvent enregistrées les unes à côté des autres. Elles peuvent être lues en une seule opération d’E/S sur disque, ce qui signifie qu’un seul accès au disque suffit pour récupérer toutes les informations nécessaires.

Restauration rapide après une panne Le fait d’utiliser un fichier journal pour garder la trace de changements récents de métadonnées ramène la vérification d’un système de fichiers à quelques secondes, même pour de très gros systèmes de fichiers.

Fiabilité via journalisation des données
ReiserFS prend également en charge la journalisation des données et les modes de données de la même façon que les concepts traités dans la section 20.2.3 page suivante. Le mode par défaut est `data=ordered` qui assure l’intégrité des données et des métadonnées à la fois, mais n’utilise la journalisation que pour les métadonnées.

20.2.2 Ext2

Les origines d’Ext2 remontent au début de l’histoire de Linux. Son prédécesseur, l’Extended File System, a été mis en œuvre en avril 1992 et intégré à Linux 0.96c. L’Extended File System a subi un certain nombre de modifications, pour devenir pendant des années le système de fichiers le plus connu sous Linux sous le nom d’Ext2. Avec l’avènement des systèmes de fichiers journalisés et leurs temps de restauration étonnamment courts, Ext2 a perdu de son importance.

Un bref résumé des points forts d’Ext2 pourrait faire comprendre pourquoi il a été — et dans une certaine mesure est encore — le système de fichiers sous Linux favori de nombreux utilisateurs de ce système d’exploitation.

Stabilité Étant véritablement un ”vénérable vieillard“, Ext2 a subi de nombreuses améliorations et a fait l’objet de tests très complets. Cela peut expliquer pourquoi le public le considère souvent ”solide comme un roc“. Après une panne de système, quand le système de fichiers ne peut pas être démonté proprement, e2fsck commence à analyser les données du système de fichiers. Les métadonnées sont remises dans un état cohérent, les fichiers ou les blocs de données en attente sont écrits dans un répertoire prévu à cet effet (nommé `lost+found`). Contrairement aux systèmes de fichiers journalisés, e2fsck analyse le système de fichiers entier et non simplement les frag-

ments de métadonnées qui viennent d'être modifiés. L'opération prend sensiblement plus de temps que la vérification d'un système de fichiers journalisé. Selon la taille du système de fichiers, cette procédure peut prendre une demi-heure, voire plus. Par conséquent, il n'est pas souhaitable de choisir Ext2 pour un serveur qui a besoin d'être toujours disponible. Toutefois, puisque Ext2 ne tient pas de journal à jour et utilise sensiblement moins de mémoire, il est parfois plus rapide que d'autres systèmes de fichiers.

Mise à niveau aisée Le code d'Ext2 constitue la base solide qui a permis à Ext3 de devenir un système de fichiers de nouvelle génération très apprécié. Sa fiabilité et sa stabilité ont été habilement combinées avec les avantages d'un système de fichiers journalisé.

20.2.3 Ext3

Ext3 a été conçu par Stephen Tweedie. Contrairement à tous les autres systèmes de fichiers de nouvelle génération, Ext3 ne suit pas un principe de conception complètement nouveau. Il est basé sur Ext2. Ces deux systèmes de fichiers sont très intimement liés entre eux. Un système de fichiers Ext3 peut très facilement être construitpar-dessus un système de fichiers Ext2. La plus grande différence entre Ext2 et Ext3 est qu'Ext3 permet la journalisation. En résumé, Ext3 offre trois avantages majeurs :

Mises à niveau aisées et extrêmement fiables à partir d'Ext2
Comme Ext3 est basé sur le code d'Ext2 et partage son format de disque ainsi que son format de métadonnées, les mises à niveau d'Ext2 vers Ext3 sont extrêmement faciles. Contrairement aux transitions vers d'autres systèmes de fichiers journalisés, tels que ReiserFS, JFS ou XFS, qui peuvent être assez fastidieuses (faires des sauvegardes du système de fichiers entier et le recréer à partir de zéro), une transition vers Ext3 n'est qu'une question de minutes. Elle est également très sûre, car recréer un système de fichiers entier à partir de zéro pourrait ne pas fonctionner parfaitement. Si l'on considère le nombre de systèmes Ext2 existants qui sont dans l'attente d'une mise à niveau vers un système de fichiers journalisé, vous pouvez aisément comprendre pourquoi Ext3 pourrait être important pour de nombreux administrateurs système. Rétrograder Ext3 en Ext2 est tout aussi facile que de mettre à niveau Ext2 en Ext3. Il suffit de démonter proprement le système de fichiers Ext3 et de le remonter en tant que système de fichiers Ext2.

Fiabilité et performance D'autres systèmes de fichiers journalisés suivent la méthode qui consiste à journaliser les "métadonnées seulement". Cela signifie que vos métadonnées sont toujours maintenues dans un état cohérent, mais que la même chose ne peut pas être automatiquement garantie pour les données du système de fichiers elles-mêmes. Ext3 est conçu pour prendre soin à la fois des métadonnées et des données. Le degré d'"attention" peut être adapté à vos préférences personnelles. Le fait d'activer Ext3 dans le mode `data=journal` offre une sécurité maximale (intégrité des données), mais peut ralentir le système car les métadonnées ainsi que les données sont consignées dans le fichier journal. Une approche relativement nouvelle consiste à utiliser le mode `data=ordered`, qui garantit à la fois l'intégrité des données et des métadonnées, mais qui n'utilise la journalisation que pour les métadonnées. Le pilote du système de fichiers rassemble tous les blocs de données qui correspondent à une mise à jour de métadonnées. Ces blocs de données écrits sur le disque avant que les métadonnées ne soient mises à jour. En conséquence, la cohérence est obtenue pour les métadonnées et les données, sans sacrifier la performance. Une troisième option à utiliser est `data=writeback`, qui permet d'écrire des données dans le système de fichiers principal, une fois ses métadonnées validées dans le fichier journal. Cette option est souvent considérée comme la meilleure en termes de performance. Elle peut cependant permettre à d'anciennes données de réapparaître dans des fichiers après une panne et une restauration, alors que la cohérence interne du système de fichiers interne est conservée. À moins que vous n'ayez spécifié une autre option, Ext3 est lancé avec le paramètre par défaut `data=ordered`.

20.2.4 Convertir un système de fichiers Ext2 en Ext3

La conversion d'un système de fichiers Ext2 en Ext3 comprend deux étapes séparées :

Créer le fichier journal Connectez-vous en tant que `root` et lancez `tune2fs -j`. Cette commande crée un journal Ext3 avec les paramètres par défaut. Pour décider vous-même de la taille qu'il devra avoir et sur quel disque il devra résider, lancez `tune2fs -J` à la place, avec les options de journal souhaitées `size=` et `device=`. D'autres informations sur le programme tune2fs se trouvent dans sa page de manuel, (tune2fs(8)).



Préciser le type de système de fichiers dans /etc/fstab
Pour vous assurer que le système de fichiers Ext3 est reconnu en tant que tel, ouvrez le fichier `/etc/fstab` et modifiez le type de système de fichiers indiqué pour la partition correspondante, de `ext2` en `ext3`. Le changement entre en vigueur au prochain réamorçage.

Utiliser Ext3 pour le répertoire racine
Pour amorcer un système de fichiers racine configuré en tant que partition Ext3, intégrez les modules `ext3` et `jbd` dans le `initrd`. Pour ce faire, modifiez le fichier `/etc/sysconfig/kernel` pour insérer les deux modules dans la ligne `INITRD_MODULES`, puis exécutez la commande `mkinitrd`.

20.2.5 Reiser4

Juste après la sortie du noyau 2.6, un nouveau membre a rejoint la famille des système de journalisation : Reiser4. Reiser4 est complètement différent de son prédecesseur ReiserFS (version 3.6). Il introduit le concept de plugins pour mettre au point les fonctionnalités du système de fichiers et un concept de sécurité à granularité plus fine.

Concept de sécurité à granularité fine
Lors de la conception de Reiser4, ses développeurs ont mis l'accent sur l'implémentation des fonctionnalités liées à la sécurité. Reiser4 contient donc un jeu de plugins spécialisés dans la sécurité. Le plus important introduit le concept d'"éléments" de fichier. À l'heure actuelle, les contrôles d'accès aux fichiers sont définis par fichier. Si un grand fichier contient des informations concernant plusieurs utilisateurs, groupes ou applications, les droits d'accès doivent être particulièrement imprécis pour inclure toutes les parties impliquées. Avec Reiser4, vous pouvez diviser ces fichiers en portions plus petites (les "éléments"). Les droits d'accès peuvent alors être attribués séparément pour chaque utilisateur permettant une gestion plus précise de la sécurité des fichiers. `/etc/passwd` en est un exemple parfait. Actuellement, seul `root` peut lire et modifier le fichier tandis que les autres utilisateurs que `root` n'ont qu'un accès en lecture à ce fichier. En utilisant le concept d'éléments de Reiser4, vous pouvez diviser le fichier en un jeu d'éléments (un élément par utilisateur) et permettre aux utilisateurs ou applications de modifier leurs propres données sans accéder aux données des autres utilisateurs. Ce concept permet une plus grande sécurité et une plus grande flexibilité à la fois.

Extensibilité avec les plugins De nombreuses fonctions de système de fichiers et de fonctions externes utilisés normalement par un système de fichiers sont implémentées en tant que plugins dans Reiser4. Ces plugins peuvent être facilement ajoutés au système de base. Il n'est plus nécessaire de recompiler le noyau ou de reformater le disque dur pour ajouter des nouvelles fonctionnalités à votre système de fichiers.

Meilleure structure du système de fichiers grâce à l'affectation différée Comme XFS, Reiser4 prend en charge l'affectation différée. Voir la section 20.2.7 page ci-contre. L'utilisation de l'affectation différée même pour les métadonnées peut résulter en une meilleure structure.

20.2.6 JFS

JFS, le *Journaling File System*, a été développé par IBM. La première version bêta du portage de JFS sous Linux a été mis à la disposition de la communauté Linux au cours de l'été 2000. La version 1.0.0 a été publiée en 2001. JFS est conçu pour répondre aux besoins des environnements serveur haut débit où les performances sont le but ultime. Étant un système de fichiers 64 bits complet, JFS prend en charge à la fois les partitions et les fichiers volumineux, ce qui constitue une autre raison de l'utiliser dans des environnements serveur.

Un examen plus détaillé de JFS montre pourquoi ce système de fichiers pourrait se révéler être un bon choix pour votre serveur Linux :

Journalisation efficace JFS suit une approche "métadonnées seulement". Au lieu d'une vérification complète, seuls sont vérifiés les changements de métadonnées générés par une activité récente du système de fichiers, ce qui économise énormément de temps lors de la restauration. Des opérations simultanées nécessitant de multiples enregistrements simultanés dans le fichier journal peuvent être combinées en une validation groupée, réduisant ainsi considérablement les baisses de performances du système de fichiers dues à de nombreuses opérations d'écriture.

Organisation efficace des répertoires JFS reste fidèle à deux organisations différentes de répertoires. Pour de petits répertoires, il permet d'enregistrer directement le contenu du répertoire dans son inode. Pour des répertoires plus volumineux, il utilise des arbres B^+, qui facilitent considérablement la gestion des répertoires.

Meilleure gestion de l'espace grâce à l'allocation dynamique des inodes
Avec Ext2, vous devez définir la densité des inodes à l'avance (l'espace occupé par les informations de gestion), ce qui restreint le nombre maximal de fichiers ou de répertoires de votre système de fichiers. JFS vous évite ces préoccupations—il alloue dynamiquement l'espace des inodes et le libère quand il n'est plus nécessaire.

20.2.7 XFS

Conçu à l'origine conçu comme le système de fichiers pour son système d'exploitation IRIX, SGI a démarré le développement de XFS au début des années 1990. L'idée derrière XFS était de créer un système de fichiers journalisé 64 bits très performant pour répondre aux défis actuels en matière d'informatique extrême. XFS est un très bon outil pour le maniement de fichiers volumineux et se comporte très bien sur du matériel de pointe. Toutefois, XFS présente un inconvénient. Comme ReiserFS, XFS accorde une grande attention à l'intégrité des métadonnées, mais moins à celle des données.

Un rapide examen des fonctionnalités clés de XFS explique pourquoi il pourrait s'avérer un concurrent de poids pour d'autres système de fichiers journalisés dans l'informatique à hautes performances.

Grande capacité à monter en charge grâce à l'utilisation de groupes d'allocation
Au moment de la création d'un système de fichiers XFS, le périphérique bloc à la base du système de fichiers est divisé en huit régions linéaires, voire plus, de taille égale. Ceux-ci sont appelés *groupes d'allocation*. Chaque groupe d'allocation gère ses propres inodes et l'espace disque libre. En pratique, on peut considérer les groupes d'allocation comme des systèmes de fichiers dans un système de fichiers. Comme les groupes d'allocation sont plutôt indépendants les uns par rapport aux autres, plusieurs d'entre eux peuvent être traités simultanément par le noyau. Cette fonctionnalité est la clé de l'excellente capacité à monter en charge de XFS. Naturellement, le principe de groupes d'allocation indépendants convient aux exigences des systèmes multiprocesseurs.

Performances élevées grâce à une gestion efficace de l'espace disque
L'espace libre et les inodes sont gérés par les arbres B^+ à l'intérieur des groupes d'allocation. Le fait d'utiliser des arbres B^+ contribue considérablement aux performances et à la capacité de montée en charge de XFS. XFS utilise l'*affectation différée*. XFS gère l'affectation en divisant le processus en

deux. Une transaction en attente est stockée dans la mémoire vive et le volume approprié d'espace est réservé. XFS ne décide pas encore de l'endroit exact (c'est-à-dire les blocs du système de fichiers) où les données devront être stockées. Cette décision est repoussée jusqu'au dernier moment possible. Certaines données temporaires ayant une durée de vie courte peuvent ne jamais être enregistrées sur le disque, car elles risquent d'être obsolètes au moment où XFS décide de l'endroit où les enregistrer. Ainsi, XFS augmente les performances en écriture et réduit la fragmentation du système de fichiers. Comme l'allocation différée entraîne des événements d'écriture moins fréquents que dans d'autres systèmes de fichiers, il est probable que la perte de données après une panne survenant au cours d'un processus d'écriture soit plus grave.

Préallocation pour éviter la fragmentation du système de fichiers
Avant d'écrire les données sur le système de fichiers, XFS *réserve* (préalloue) l'espace libre nécessaire pour un fichier. La fragmentation du système de fichiers est ainsi considérablement réduite. Les performances sont améliorées, car le contenu d'un fichier n'est pas réparti sur la totalité du système de fichiers.

20.3 Autres systèmes de fichiers pris en charge

Le tableau 20.1 de la présente page résume quelques autres système de fichiers pris en charge par Linux. Ils le sont principalement pour assurer la compatibilité et l'échange de données avec différentes sortes de supports ou des systèmes d'exploitation différents.

TAB. 20.1: *Types de systèmes de fichiers sous Linux*

`cramfs`	*Compressed ROM file system* : un système de fichiers compressé en lecture seule pour les mémoires mortes (ROM).
`hpfs`	*High Performance File System* : le système de fichiers standard IBM OS/2 — uniquement pris en charge en mode lecture seule.
`iso9660`	Système de fichiers standard des CD-ROM.

`minix`	Ce système de fichiers est issu de projets universitaires sur les systèmes d'exploitation et est le premier système d'exploitation utilisé sous Linux. Aujourd'hui, il sert de système de fichiers pour les disquettes.
`msdos`	*fat*, le système de fichiers employé à l'origine par DOS, est aujourd'hui utilisé par divers systèmes d'exploitation.
`ncpfs`	Système de fichiers utilisé pour monter des volumes Novell en réseau.
`nfs`	*Network File System* : ici, les données peuvent être enregistrées sur n'importe quelle machine d'un réseau et on y accédera en réseau.
`smbfs`	*Server Message Block* est utilisé par des produits tels que Windows pour permettre l'accès en réseau aux fichiers.
`sysv`	Utilisés sous SCO UNIX, Xenix et Coherent (des systèmes UNIX commerciaux pour PC).
`ufs`	Utilisé par BSD, SunOS et NeXTstep. Pris en charge uniquement en mode lecture seule.
`umsdos`	*UNIX on MSDOS* : appliqué en plus d'un système de fichiers `fat` normal, permet d'obtenir les fonctionnalités offertes par UNIX (droits d'accès, liens, noms de fichiers longs) grâce à la création de fichiers spéciaux.
`vfat`	*Virtual FAT* : extension du système de fichiers `fat` (prend en charge les noms de fichiers longs).
`ntfs`	*Windows NT file system*, lecture seule.

20.4 Prise en charge des fichiers volumineux sous Linux

À l'origine, Linux prenait en charge une taille maximale de fichier de 2 Go. C'était suffisant avant l'explosion du multimédia et tant que personne n'essayait de manipuler d'énormes bases de données sous Linux. Devenant de plus en plus importants pour l'informatique serveur,le noyau et la bibliothèque C ont été modifiés de façon à prendre en charge des tailles de fichiers supérieures à 2 Go grâce

à un nouvel ensemble d'interfaces que les applications doivent utiliser. Aujourd'hui, pratiquement tous les systèmes de fichiers les plus importants permettent d'utiliser LFS, ce qui ouvre une porte vers l'informatique à hautes performances. Le tableau 20.2 de la présente page propose un survol des limitations actuelles des fichiers et systèmes de fichiers sous Linux.

TAB. 20.2: *Tailles maximales des systèmes de fichiers (format sur disque)*

Système de fichiers	**Taille du fichier (octets)**	**Taille du système de fichiers (octets)**
Ext2 ou Ext3 (blocs d'une taille de 1 ko)	2^{34} (16 Go)	2^{41} (2 To)
Ext2 ou Ext3 (blocs d'une taille de 2 ko)	2^{38} (256 Go)	2^{43} (8 To)
Ext2 ou Ext3 (blocs d'une taille de 4 ko)	2^{41} (2 To)	2^{44} (16 To)
Ext2 ou Ext3 (blocs d'une taille de 8 ko) (systèmes ayant des pages de 8 ko, comme Alpha)	2^{46} (64 To)	2^{45} (32 To)
ReiserFS v3	2^{46} (64 Go)	2^{45} (32 To)
XFS	2^{63} (8 Eo)	2^{63} (8 Eo)
JFS (blocs d'une taille de 512 octets)	2^{63} (8 Eo)	2^{49} (512 To)
JFS (blocs d'une taille de 4 ko)	2^{63} (8 Eo)	2^{52} (4 Po)
NFSv2 (côté client)	2^{31} (2 Go)	2^{63} (8 Eo)
NFSv3 (côté client)	2^{63} (8 Eo)	2^{63} (8 Eo)

Important

Limitations du noyau Linux

Le tableau 20.2 page précédente décrit les limitations concernant le format de disque. Le noyau 2.6 impose ses propres limites de la taille des fichiers et des systèmes de fichiers qu'il gère :

Taille de fichier Sur les systèmes 32 bits, les fichiers ne peuvent pas dépasser la taille de 2 To (2^{41} octets).

Taille du système de fichiers Les systèmes de fichiers peuvent atteindre une taille jusqu'à 2^{73} octets). Cependant, cette limite est encore hors de portée du matériel sur le marché.

Important

20.5 Pour plus d'informations

Chacun des projets de systèmes de fichiers décrit ci-dessus possède son propre site web sur lequel vous trouverez des informations extraites de listes de discussion, de la documentation additionnelle et des FAQ.

- `http://e2fsprogs.sourceforge.net/`
- `http://www.zipworld.com.au/~akpm/linux/ext3/`
- `http://www.namesys.com/`
- `http://oss.software.ibm.com/developerworks/opensource/jfs/`
- `http://oss.sgi.com/projects/xfs/`

Un tutoriel complet en plusieurs parties sur les systèmes de fichiers Linux est présent sur le site *IBM developerWorks* à l'adresse suivante : `http://www-106.ibm.com/developerworks/library/l-fs.html`. Une comparaison des différents systèmes de fichiers journalisés sous Linux réalisée par Juan I. Santos Florido pour la *Linux Gazette* est disponible à l'adresse suivante : `http://www.linuxgazette.com/issue55/florido.html`. Les personnes intéressées par une analyse approfondie de LFS sous Linux peuvent consulter le site sur LFS d'Andreas Jaeger à l'adresse suivante : `http://www.suse.de/~aj/linux_lfs.html`.

Authentification avec PAM

PAM (en anglais, Pluggable Authentication Modules) est utilisé sous Linux pour la communication entre les utilisateurs et les applications lors de l'authentification. Les modules PAM sont disponibles centralement et peuvent être appelés de chaque application. Le contenu de ce chapitre a pour but de montrer comment cette authentification modulaire se configure et comment elle fonctionne.

Les administrateurs et les développeurs désirent limiter l'accès à des domaines spécifiques du système ou l'utilisation de certaines fonctions d'une application. Sans PAM, il faudrait adapter chaque application à toute nouvelle méthode d'authentification telle que LDAP ou Samba. Cette façon de faire coûte cher en temps et augmente les risques d'erreur. L'idée est donc de séparer l'authentification de l'application et de la déléguer à un module central : cela permet d'éviter ces inconvénients. Si une nouvelle méthode d'authentification doit être mise en oeuvre, il suffit d'adapter ou de développer un module PAM que l'application peut utiliser.

Il existe un fichier de configuration propre pour chaque programme qui utilise PAM, sous `/etc/pam.d/<service>`.

On détermine dans ce fichier la liste du ou des modules PAM utilisés pour l'authentification des utilisateurs. Une configuration globale de la plupart des modules PAM se trouve sous `/etc/security` et détermine le comportement exact du module concerné (par exemple, `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf` et `time.conf`). Une application qui utilise un module PAM appelle une séquence de fonctions PAM qui traitent les informations des divers fichiers de configuration et transmettent le résultat à l'application.

21.1 Structure d'un fichier de configuration PAM

Chaque ligne d'un fichier de configuration PAM contient un maximum de quatre colonnes :

```
<Type de module> <Fanion de contrôle> <Chemin du module> <Options>
```

Les modules PAM sont traités en pile. Les divers modules ont des tâches différentes. Un module se charge de la vérification des mots de passe, un autre vérifie la provenance d'un accès et un autre interroge des paramètres spécifiques à l'utilisateur. PAM connaît quatre type de modules :

`auth` Les modules de ce type servent à vérifier si l'utilisateur est authentifié. Cette vérification se fait traditionnellement par une demande de mot de passe, mais peut également s'effectuer par carte à puce ou par des informations biométriques (empreintes digitales, rétinienne, etc).

account Les modules de ce type vérifient si l'utilisateur est autorisé à utiliser le service demandé. Par exemple, personne ne devrait pouvoir se connecter à un système alors que son compte a expiré.

password Les modules de ce type servent à la modification des données d'authentification. Dans la plupart des cas, il s'agit d'un mot de passe.

session Les modules de ce type servent à l'administration et à la configuration de sessions utilisateur. Ces modules sont activés avant et après l'authentification, de manière à journaliser les tentatives de connexion et à configurer l'environnement de l'utilisateur (chemin d'accès au courrier électronique, répertoire personnel, limites systèmes, etc).

La deuxième colonne contient un indicateur de contrôle qui influence le comportement des modules démarrés :

required L'authentification ne peut continuer que si le module réussit son exécution. En cas d'erreur lors de l'exécution d'un module ayant l'indicateur `required`, les autres modules sont également exécutés, avant que les utilisateurs ne reçoivent l'information que la tentative d'authentification n'a pas aboutit.

requisite Les modules doivent réussir leur exécution de la même manière que dans le cas de `required`. Cependant, lors d'une erreur, l'échec est immédiatement communiqué à l'utilisateur sans exécuter d'autres modules. En cas de succès, les modules suivants sont exécutés de la même manière que dans le cas de `required`. Cet indicateur peut servir de filtre simple, de manière à garantir que toutes les conditions requises pour une authentification correcte soient nécessaires.

sufficient Si un module de ce type s'exécute avec succès, le programme appelant obtient immédiatement l'information que l'authentification a réussi et aucun autre module n'est exécuté, dans la mesure où aucun module précédemment exécuté sans succès ne portait l'indicateur `required`. Si l'exécution d'un module ayant l'indicateur `sufficient` est sans succès, cela n'a aucune conséquence directe, les modules suivants sont simplement traités dans l'ordre.

optional La réussite ou l'échec n'a pas d'effet. Cette propriété peut être par exemple utilisé pour un module qui n'est destiné qu'à afficher des messages (par exemple, informer l'utilisateur de la réception d'un courrier électronique) et ne procède à aucune autre action.

include Si cet indicateur est présent, le fichier spécifié en tant qu'argument est inséré ici.

Le chemin du module n'est pas spécifié s'il réside dans le répertoire par défaut `/lib/security` (respectivement sous `/lib64/security` pour toutes les plateformes 64 bits prises en charge par SUSE LINUX). La quatrième colonne peut contenir une option du module, comme par exemple `debug` (mode de débogage) ou `nullok` (permet l'utilisation de mots de passe vides).

21.2 La configuration PAM de sshd

Après la théorie de la configuration PAM, vous trouverez ici un exemple pratique, la configuration PAM de sshd :

Example 21.1: *Configuration PAM de sshd*

```
#%PAM-1.0
auth     include        common-auth
auth     required       pam_nologin.so
account  include        common-account
password include        common-password
session  include        common-session
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README.SuSE)
#session  optional      pam_resmgr.so fake_ttyname
```

La configuration PAM typique d'une application (sshd dans le cas présent) contient quatre déclarations qui font référence aux fichiers de configuration de quatre types de modules : `common-auth`, `common-account`, `common-password`, et `common-session`. Ces quatre fichiers contiennent la configuration par défaut de chaque type de module. En les incluant plutôt qu'en faisant appel à chaque module séparément pour chaque application PAM, vous obtenez automatiquement une configuration PAM mise à jout si l'administrateur change les paramètres par défaut. Par le passé, vous deviez ajuster tous les fichiers de configuration manuellement pour toutes les applications lorsque des modifications étaient apportées à PAM ou quand une nouvelle application était installée. La configuration PAM et toutes les modifications qui lui sont apportées sont transmis à travers les fichiers de configuration par défaut.

Le premier fichier inclus (`common-auth`) appelle deux modules du type `auth` : `pam_env` et `pam_unix2`. Voir l'exemple 21.2 page ci-contre.

Example 21.2: Configuration par défaut de la section `auth`

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

Le premier module, `pam_env`, charge le fichier `/ect/security/pam_env.conf` pour définir les variables d'environnement telles qu'elles sont spécifiées dans le fichier. Ceci peut être utilisé pour configurer la variable `DISPLAY` à la bonne valeur, car le module `pam_env` sait d'où l'utilisateur tente de se connecter. Le second module, `pam_unix2`, vérifie le login (nom) et le mot de passe de l'utilisateur à l'aide de `/etc/passwd` et de `/etc/shadow`.

Une fois que les modules spécifiés dans `common-auth` ont été appelés avec succès, un troisième module appelé `pam_nologin` vérifie si le fichier `/etc/nologin` existe. Dans ce cas, à part `root`, aucun utilisateur n'a permission d'accès. La "pile" (en anglais stack) complète des modules `auth` est traitée avant que le démon ssh obtienne une réponse quant à la réussite de l'authentification. Tous les modules portent donc un indicateur de contrôle `required` et doivent donc être tous traités avant que la réussite soit communiquée à sshd. En cas d'échec d'un de ces modules, le résultat final communiqué sera négatif, mais sshd ne l'apprendra que lorsque tous la pile de modules aura été traitée.

Dès que les modules spécifiés dans `auth` ont été traités avec succès, une autre déclaration incluse est traitée ; dans le cas présent, celui dans l'exemple 21.3 de la présente page. `common-account` ne contient qu'un module, `pam_unix2`. Si `pam_unix2` informe que l'utilisateur existe, sshd reçoit un message annonçant ce succès et la pile de modules suivante (`password`) est traitée comme décrit dans l'exemple 21.4 de la présente page.

Example 21.3: Configuration par défaut de la section `account`

```
account required        pam_unix2.so
```

Example 21.4: Configuration par défaut de la section `password`

```
password required       pam_pwcheck.so  nullok
password required       pam_unix2.so    nullok use_first_pass use_authtok
#password required      pam_make.so     /var/yp
```

Encore une fois, la configuration PAM de sshd n'implique qu'une déclaration faisant référence à la configuration par défaut pour des modules `password` situés dans `common-password`. Ces modules doivent être traités avec succès (indicateur de contrôle `required`) lorsque l'application change les données d'authentification. La modification d'un mot de passe ou d'une autre donnée d'authentification requiert la vérification de la sécurité ce qui est réalisé à l'aide du module PAM `pam_pwcheck`. Le module `pam_unix2`, utilisé par la suite, prend les anciens et nouveaux mots de passe de `pam_pwcheck`. L'utilisateur ne doit donc pas s'identifier à nouveau. De plus, on évite de passer outre les contrôles de `pam_pwcheck`. Les modules de type `password` devraient toujours être exécutés dans la mesure où les modules précédents de type `account` ou `auth` avertissent d'un mot de passe périmé.

Example 21.5: *Configuration par défaut de la section* `session`

```
session required        pam_limits.so
session required        pam_unix2.so
```

Enfin, les modules de type `session`, rassemblés dans le fichier `common-session`, sont appelés de manière à configurer la session pour cet utilisateur de la façon prévue. Le module `pam_unix2` est appelé à nouveau, sans effet en pratique en raison de l'option `none` spécifiée dans le fichier de configuration respectif de ce module, `pam_unix2.conf`. Le module `pam_limits` charge le fichier `/etc/security/limits.conf` qui définit les limites d'utilisation de certaines ressources systèmes. Lorsque l'utilisateur se déconnecte, les modules de type `session` sont à nouveau appelés.

21.3 Configuration des modules PAM

Certains modules PAM sont configurables. Les fichiers de configuration correspondants se trouvent sous `/etc/security`. Cette section décrit brièvement les fichiers utilisés dans l'exemple de sshd—`pam_unix2.conf`, `pam_env.conf`, `pam_pwcheck.conf` et `limits.conf`.

21.3.1 pam_unix2.conf

Pour l'authentification traditionnelle par mot de passe, le module PAM pam_unix2 est utilisé. Il lit ses données de /etc/passwd, /etc/shadow, de tables NIS ou NIS+, ou d'une base de données LDAP. On peut configurer ce module soit individuellement dans la configuration PAM de l'application, ou globalement dans /etc/security/pam_unix2.conf. Dans le cas le plus simple, le fichier de configuration du module est tel que l'exemple 21.6 de la présente page.

Example 21.6: *pam_unix2.conf*

```
auth:   nullok
account:
password:       nullok
session:        none
```

L'option nullok, pour les types de modules auth et password, signifie que des mots de passe vides sont admis pour ce type de compte. L'utilisateur a le droit de changer les mots de passe. On demande à l'aide de l'option none pour le type de module session qu'aucun message ne soit journalisé (configuration standard). Vous pouvez obtenir d'autres options de configuration dans ce fichier ou dans la page de manuel de pam_unix2(8).

21.3.2 pam_env.conf

Ce fichier peut être utilisé pour donner un environnement standardisé aux utilisateurs, via l'appel du module pam_env. Avec lui, définissez des variables d'environnement en utilisant la syntaxe suivante :

```
VARIABLE  [DEFAULT=[valeur]]  [OVERRIDE=[valeur]]
```

VARIABLE Désignation de la variable d'environnement qui doit être assignée

[DEFAULT=[valeur]] Valeur standard configurée par l'administrateur (utilisée par défaut)

[OVERRIDE=[valeur]] Valeurs qui peuvent être déterminées par pam_env et assignées à la place de la valeur standard

Un exemple courant pour lequel la valeur par défaut devrait être écrasée par `pam_env` est la variable`DISPLAY` qui est changée lors de chaque connexion distante. Voir l'exemple 21.7 de la présente page.

Example 21.7: *pam_env.conf*

```
REMOTEHOST     DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY        DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

La première ligne configure la valeur `localhost` à la variable `REMOTEHOST`. Celle-ci est utilisée lorsque `pam_env` ne peut pas déterminer d'autres valeurs. La variable `DISPLAY` contient la valeur de la variable `REMOTEHOST`. Vous trouverez plus d'informations dans les commentaires situés dans le fichier `/etc/security/pam_env.conf`.

21.3.3 pam_pwcheck.conf

Le module `pam_pwcheck` cherche dans ce fichier les options de tous les modules de type `password`. Les configurations stockées ici sont lues avant celles des configurations de l'application. Si l'application n'a pas de configuration spécifique, les configurations globales sont utilisées. L'exemple 21.8 de la présente page informe `pam_pwcheck` d'autoriser les mots de passe vides et la modification des mots de passe. Vous trouverez plus d'options pour le module dans le fichier `/etc/security/pam_pwcheck.conf`.

Example 21.8: *pam_pwcheck.conf*

```
password:    nullok
```

21.3.4 limits.conf

Le module `pam_limits` configure les limites systèmes pour des utilisateurs ou groupes spécifiques depuis le fichier `limits.conf`. Théoriquement, on peut configurer dans ce fichier des limites dures, sans dépassement possible, et molles, où des dépassement temporaires sont possibles. Vous trouverez des informations sur la syntaxe et les options possibles directement dans le fichier.

21.4 Informations complémentaires

Sur votre système, vous trouverez dans le répertoire `/usr/share/doc/packages/pam` les documentations suivantes :

README Au plus haut niveau de ce répertoire se trouvent des README généraux. Dans le sous-répertoire `modules` vous trouverez des README traitant des modules PAM disponibles.

The Linux-PAM System Administrators' Guide Tout ce qu'un administrateur système doit savoir sur PAM. Vous trouverez ici des thèmes comme la syntaxe d'un fichier de configuration PAM ou les aspects de sécurité sous PAM. Ce document est disponible dans les formats PDF, HTML ou texte.

The Linux-PAM Module Writers' Manual Vous trouverez ici les informations dont le développeur a besoin pour écrire des modules PAM conformes aux standards. Ce document est disponible dans les formats PDF, HTML ou texte.

The Linux-PAM Application Developers' Guide Ce document contient tout ce qu'un développeur d'application désireux d'utiliser les bibliothèques PAM doit savoir. Ce document est disponible dans les formats PDF, HTML ou texte.

Thorsten Kukuk a développé nombre de modules PAM pour SUSE LINUX et il met à votre disposition certaines informations sous : `http://www.suse.de/~kukuk/pam/`.

Troisième partie

Services

Bases de la mise en réseau

Linux, en véritable enfant de l'Internet, vous offre tous les outils et toutes les fonctionnalités pour s'intégrer à tous les types de structures réseau. Nous traiterons du protocole classique utilisé sous Linux, TCP/IP, qui propose de nombreux services et particularités. Vous pouvez configurer un accès au réseau avec une carte réseau, un modem ou un autre périphérique grâce à YaST. Vous pouvez également le configurer à la main. Nous ne traiterons dans ce chapitre que des mécanismes fondamentaux et les fichiers de configuration réseau correspondants.

Linux et les autres systèmes d'exploitation Unix utilisent le protocole TCP/IP. Ce n'est pas un protocole réseau unique mais plutôt une famille de protocoles réseau qui offrent différents services. Les protocoles énumérés dans le tableau 22.1 de la présente page permettent d'échanger des données entre deux ordinateurs par TCP/IP. "L'Internet" fait référence à l'ensemble des réseaux combinés par TCP/IP, y compris un réseau mondial.

RFC signifie Request for Comments (Demande de Commentaires). Les documents RFC décrivent les différents protocoles Internet et les procédures d'implantation pour le système d'exploitation et ses applications. Les documents RFC décrivent la construction des protocoles Internet. Pour approfondir vos connaissances à propos d'un protocole particulier, référez-vous aux documents RFC correspondant. Ils sont disponibles en ligne à l'adresse `http://www.ietf.org/rfc.html`.

TAB. 22.1: *Différents protocoles de la famille de protocoles TCP/IP*

Protocole	Description
TCP/IP	(en anglais Transmission Control Protocol). Un protocole sûr, orienté connexion. Les données à transmettre sont, du point de vue de l'application, envoyées sous forme de flux de données et c'est le système d'exploitation lui-même qui les met au format de transport adapté. Les données arrivent dans l'application cible, sur l'ordinateur cible, exactement sous la forme du flux de données dans lequel elles ont été envoyées. Le protocole TCP permet de garantir qu'aucune donnée n'est perdue ou n'arrive dans le désordre. Ce protocole est utilisé quand l'ordre des données est important et que le terme 'connexion' a un sens.
DNS	(en anglais, User Datagram Protocol). Un protocole sans connexion, non sûr. Les données à transmettre sont envoyées par paquets, ces paquets de données étant générés, au préalable, par l'application. L'ordre d'arrivée des données chez le destinataire n'est pas garanti et il se peut aussi que certains paquets de données soient perdus. Le protocole UDP est particulièrement adapté pour les applications orientées trames et se caractérise par des temps morts inférieurs à ceux du protocole TCP.

ICMP	(en anglais, Internet Control Message Protocol) C'est un protocole qui n'est en général pas destiné à l'utilisateur, il s'agit plutôt d'un protocole de contrôle spécial qui transmet les états d'erreur et qui peut piloter le comportement de l'ordinateur en charge de la transmission de données TCP/IP. Il fournit en outre un mode écho spécial que vous pouvez tester avec le programme ping.
IGMP	(en anglais, Internet Group Management Protocol) Ce protocole contrôle le comportement des ordinateurs dans le cadre de la multidiffusion IP.

Comme décrit dans la figure 22.1 de la présente page, l'échange de données a lieu au niveau de différentes couches. La couche de communication en soi est le transfert de données non sûre à travers le protocole IP (en anglais, Internet Protocol). Greffé sur IP, le protocole TCP (en anglais, Transmission Control Protocol) garantit, dans une certaine mesure, une transmission sûre des données. La couche IP est prise en charge par le protocole dépendant du matériel sous-jacent, par exemple ethernet.

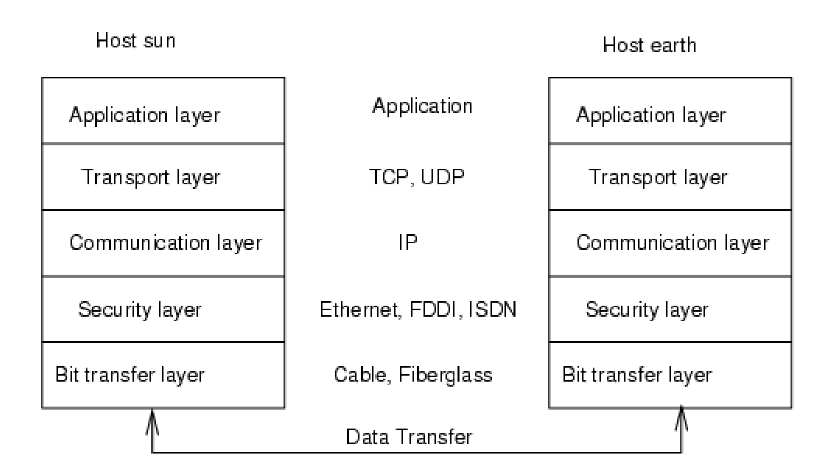


FIG. 22.1: *Modèle en couches simplifié pour TCP/IP*

L'illustration montre un ou deux exemples pour chaque couche. Comme vous pouvez le voir, les couches sont classées par *niveau d'abstraction*, la couche inférieure étant la plus proche du matériel. La couche supérieure, en revanche, fait pratiquement intégralement abstraction du matériel sous-jacent. Chacune des couches a une fonction bien particulière, déjà décrite en grande partie par son nom. C'est ainsi que le réseau utilisé (par exemple Ethernet) est représenté par la couche physique et par la couche liaison.

Presque tous les protocoles matériel sont orientés paquets. Les données à transmettre doivent être placées dans des *paquets* car elles ne peuvent pas être envoyées en une fois. La taille maximale d'un paquet TCP/IP est d'environ 64 Ko. En pratique, les paquets sont généralement plus petits, dans la mesure où le matériel réseau est le facteur limitatif. Ainsi la taille maximale autorisée d'un paquet de données sur Ethernet est de 1 500 octets. C'est donc pour cette raison que la taille des paquets TCP/IP est limitée lorsque les données sont envoyées sur un réseau Ethernet. Lorsque l'on souhaite transmettre davantage de données, le système d'exploitation doit envoyer davantage de paquets de données.

Pour que les couches puissent exécuter les tâches qui leur reviennent, des informations supplémentaires relatives à chaque couche doivent être enregistrées dans les paquets de données, au niveau de l'*en-tête*. Chacune des couches ajoute un petit bloc de données, appelé en-tête de protocole (en anglais, protocol header) au début du paquet en formation. Un paquet de données TCP/IP quelconque en route sur un câble Ethernet est illustré en la figure 22.2 de la présente page. La somme de contrôle se trouve à la fin du paquet et non au début. Cela simplifie les choses pour le matériel réseau.

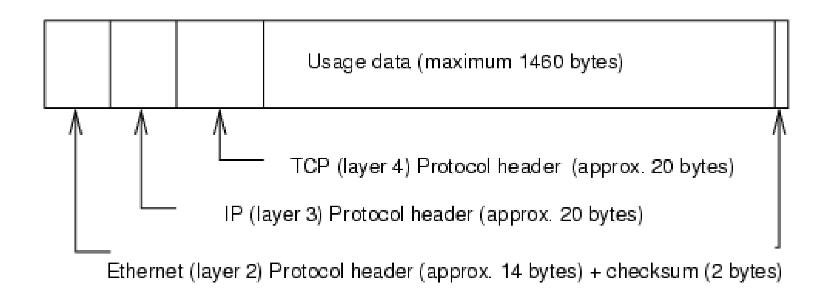


FIG. 22.2: *Paquet TCP/IP sur Ethernet*

Ainsi, si une application souhaite envoyer des données sur le réseau, les données passent au travers des différents niveaux de couches, tous mis en œuvre au sein du noyau Linux à l'exception de la couche 1 (la carte réseau). Chacune des couches est responsable de préparer les données de manière à ce qu'elles puissent être transmises à la couche suivante. La couche la plus basse est, au final, responsable de l'envoi des données à proprement parler. Le processus est inversé lorsque des données sont reçues. Un peu comme pour les différentes peaux d'un oignon, les en-têtes de protocole de chaque couche sont retirés, au fur et à mesure, des données utiles. La couche 4 est, au final, responsable de la préparation des données pour les applications sur l'ordinateur cible. Ainsi, une couche ne communique jamais qu'avec la couche directement au-dessus ou en dessous d'elle. Le fait que les données sont transmises par un réseau FDDI 100 Mbit/s ou une connexion 56 Kbit/s n'a pas d'importance pour les applications. De même, la nature des données envoyées importe peu pour la connexion de données tant qu'elles sont correctement empaquetées.

22.1 Adresses IP et routage

Les sections suivantes se limitent aux réseaux IPv4. Vous trouverez des informations sur son successeur, le protocole IPv6, à la section 22.2 page 423.

22.1.1 Adresses IP

Chaque ordinateur de l'Internet possède une adresse 32 bits unique. Ces 32 bits (soit 4 octets) se présentent normalement comme dans la seconde ligne de l'exemple 22.1 de la présente page.

Example 22.1: *Structure d'une adresse IP*

```
Adresse IP (binaire):  11000000 10101000 00000000 00010100
Adresse IP (décimale):      192.     168.       0.      20
```

Les quatre octets sont séparés par un point lorsqu'ils sont écrits dans le système décimal. L'adresse IP est associée à un ordinateur ou à une interface réseau, elle ne peut donc être utilisée nulle part ailleurs dans le monde. Certes il existe des exceptions à cette règle, mais elles n'ont aucune influence sur les considérations suivantes.

La carte Ethernet aussi possède une adresse non équivoque, appelée adresse *MAC* (en anglais, Media Access Control, contrôle d'accès au support). Cette adresse se compose de 48 bits, est unique dans le monde entier et est enregistrée physiquement par le fabricant directement sur la carte réseau. L'attribution de l'adresse par le fabricant présente toutefois un inconvénient non négligeable — les adresses *MAC* ne constituent pas un système hiérarchique, mais sont au contraire réparties de manière plus ou moins aléatoire. Elles ne peuvent donc pas servir à adresser un ordinateur distant. L'adresse *MAC* joue en revanche un rôle décisif lors de la communication entre les ordinateurs d'un réseau local et il s'agit de l'élément principal de l'en-tête de protocole de la couche 2.

Revenons aux adresses IP : les points suggèrent que les adresses IP constituent un système hiérarchique. Jusque dans les années 90, les adresses IP étaient réparties en classes, de manière fixe. Ce système s'est toutefois révélé particulièrement rigide et c'est pour cette raison que l'on a abandonné cette répartition. On utilise désormais un "routage ne faisant pas appel à des classes" (CIDR, en anglais, Classless Inter Domain Routing).

22.1.2 Masques réseau et routage

Comme l'ordinateur avec l'adresse IP 192.168.0.1 ne peut tout simplement pas savoir où se trouve l'ordinateur avec l'adresse IP 192.168.0.20, il a fallu introduire les masques réseau. Pour simplifier, les masques de (sous)-réseau définissent, sur un ordinateur disposant d'une adresse IP, ce qui se trouve "à l'intérieur" et ce qui se trouve "à l'extérieur". Les ordinateurs qui se trouvent "à l'intérieur" (les spécialistes disent : "sur le même sous-réseau"), peuvent être adressés directement. Les ordinateurs qui se trouvent "à l'extérieur" ("pas sur le même sous-réseau"), doivent être adressés par l'intermédiaire d'une passerelle ou d'un routeur. Comme chaque interface réseau est susceptible de posséder sa propre adresse IP, vous imaginez comme tout cela peut vite devenir compliqué.

Voilà ce qui se produit, avant l'envoi d'un paquet sur le réseau : on combine l'adresse cible et le masque réseau au moyen d'un ET binaire. On combine aussi l'adresse source et le masque réseau au moyen d'un ET binaire. Lorsque plusieurs interfaces réseau sont disponibles, toutes les adresses d'envoi possibles sont, en règle générale, vérifiées. Les résultats des combinaisons au moyen de ET binaires sont comparés. Si les résultats sont rigoureusement identiques, cela signifie que l'ordinateur cible se trouve dans le même sous-réseau. Dans le cas contraire, il faut y accéder par l'intermédiaire d'une passerelle. Plus il y a de bits à "1" dans le masque réseau, moins il est possible d'adresser de machines directement et plus il faudra passer par une passerelle pour accéder à des hôtes distants.

Vous pouvez consulter les différents exemples illustrés dans le exemple 22.2 de la présente page.

Example 22.2: *Rattachements des adresses IP avec le masque réseau*

```
Adresse IP (192.168.0.20) :  11000000 10101000 00000000 00010100
Masque réseau   (255.255.255.0) :  11111111 11111111 11111111 00000000
---------------------------------------------------------------
Résultat du lien :         11000000 10101000 00000000 00000000
Dans le système décimal :           192.     168.       0.       0

Adresse IP (213.95.15.200) : 11010101 10111111 00001111 11001000
Masque réseau    (255.255.255.0) : 11111111 11111111 11111111 00000000
---------------------------------------------------------------
Résultat du lien :         11010101 10111111 00001111 00000000
Dans le système décimal :           213.      95.      15.       0
```

Les masques réseau, comme les adresses IP,s'écrivent sous forme de nombres décimaux, séparés par des points. Comme le masque réseau est également une valeur 32 bits, on l'exprime sous la forme d'une suite de quatre valeurs décimales. Il faut indiquer quelle passerelle et quel domaine d'adresses sont accessibles par l'intermédiaire de quelle interface réseau.

Un autre exemple : tous les ordinateurs raccordés au même câble Ethernet se trouvent, en règle générale, *sur le même sous-réseau* et sont directement accessibles. Même si le brin Ethernet est segmenté par des commutateurs ou des ponts, ces ordinateurs demeurent toujours directement accessibles.

Si vous souhaitez parcourir une plus longue distance, la technologie Ethernet économique n'est alors plus appropriée. Vous devez alors confier les paquets IP à d'autres types de matériels, comme FDDI ou RNIS. Des appareils de ce type s'appellent des routeurs ou des passerelles. Une machine Linux peut bien entendu aussi se charger de ce genre de tâches. L'option correspondante est intitulée `ip_forwarding`.

Lorsqu'au moins une passerelle est configurée, le paquet IP est envoyé à la passerelle appropriée. Cette dernière essaie alors de nouveau d'envoyer ce paquet selon le même schéma —d 'hôte en hôte — jusqu'à ce que le paquet ait atteint l'ordinateur cible ou que son TTL (en anglais, time to live, durée de vie) soit écoulé.

TAB. 22.2: *Adresses spéciales*

Type d'adresse	Description
Adresse de base du réseau	Il s'agit du masque réseau ET d'une adresse quelconque du réseau, comme illustré dans l'exemple 22.2 page précédente sous `Résultat`. Cette adresse ne peut être attribuée à aucun ordinateur.
Adresse de diffusion (broadcast)	Elle signifie : "s'adresser à tous les ordinateurs de ce sous réseau". Pour la produire, le masque réseau est inversé binairement et combiné à l'adresse de base réseau avec un OU. L'exemple ci-dessus permet donc d'obtenir 192.168.0.255. Bien entendu, cette adresse ne peut non plus être attribuée à aucun ordinateur.
Hôte local	L'adresse `127.0.0.1` est attribuée, sur chaque ordinateur, de manière fixe, à ce que l'on appelle le "dispositif de bouclage". Cette adresse peut permettre d'établir une connexion avec l'ordinateur lui-même.

Comme les adresses IP doivent être uniques à l'échelle mondiale, vous ne pouvez naturellement pas choisir des adresses quelconques. Mais pour que vous puissiez tout de même mettre au point un réseau IP, il existe trois domaines d'adresses que vous pouvez utiliser sans plus de formalités. Vous ne pouvez pas les utiliser telles quelles sur l'Internet, car ces adresses ne sont pas acheminées sur l'Internet. Ces domaines d'adresses sont spécifiés dans la RFC 1597 et sont énumérés dans le tableau 22.3 de la présente page.

TAB. 22.3: *Domaines d'adresses IP privés*

Réseau/Masque réseau	Domaine
`10.0.0.0/255.0.0.0`	`10.x.x.x`
`172.16.0.0/255.240.0.0`	`172.16.x.x - 172.31.x.x`
`192.168.0.0/255.255.0.0`	`192.168.x.x`

22.2 IPv6 — L'Internet de nouvelle génération

Avec l'invention du WWW (World Wide Web), l'Internet et donc le nombre d'ordinateurs qui communiquent via TCP/IP ont connu une croissance exponentielle dans les quinze dernières années. Depuis que Tim Berners-Lee a inventé le WWW en 1990 au CERN (`http://public.web.cern.ch/`), le nombre des machines sur Internet est passé de quelques milliers à environ 100 millions.

Comme vous le savez déjà, une adresse IP ne contient que 32 bits. De nombreuses adresses IP ne peuvent, pour des raisons d'organisation des réseaux, pas être utilisées et sont donc perdues. Vous disposez dans votre sous-réseau d'un nombre d'adresses égal à deux élevé à la puissance du nombre de bits, moins deux. Un sous-réseau se compose alors, par exemple de 2, 6 ou 14 adresses. Si vous souhaitez par exemple connecter 128 ordinateurs à l'Internet, vous aurez donc besoin d'un sous-réseau comportant 256 adresses IP, dont 254 sont utilisables car deux adresses sont nécessaires à la structure du sous-réseau, à savoir l'adresse de diffusion et l'adresse de base du réseau.

Pour atténuer la pénurie prévisible d'adresses, on utilise sous le protocole IPv4 momentanément utilisé des mécanismes tels que le DHCP ou le NAT (en anglais, Network Address Translation). Ces deux processus permettent d'atténuer, avec la convention des domaines d'adresses privés et publics le besoin urgent d'adresses Internet. L'inconvénient de ces méthodes est qu'elles sont relativement compliquées à configurer et nécessitent une maintenance considérable. Elles impliquent de connaître, pour la configuration correcte d'un ordinateur sur un réseau IPv4, de nombreuses informations, notamment, sa propre adresse IP, son masque de sous-réseau, l'adresse de la passerelle et impérativement un serveur de noms. Vous devez "connaître" toutes ces informations et ne pouvez les déduire d'aucune autre donnée.

Avec IPv6, la pénurie d'adresses et les configurations complexes appartiennent désormais au passé. Vous allez, dans les sections suivantes, en apprendre davantage sur les nouveautés et les avantages d'IPv6 et sur le passage de l'ancien protocole au nouveau.

22.2.1 Avantages

L'avantage le plus important et le plus évident de ce nouveau protocole est qu'il augmente de façon énorme l'espace d'adresses disponibles. Une adresse IPv6

comprend 128 bits contre 32 bits jusqu'alors. On dispose alors de plusieurs milliards (!) d'adresses IP.

Les adresses IPv6 diffèrent des anciennes, non seulement par leur longueur, mais également par leur structure interne différente et permettent de coder des informations spéciales relatives au système correspondant et à son réseau. Vous trouverez plus d'informations à ce sujet à la section 22.2.2 page ci-contre.

D'autres avantages significatifs du nouveau protocole, en bref :

Auto-configuration IPv6 transpose le principe du "Plug and Play" au réseau. Un système fraîchement installé s'intègre au réseau (local) sans qu'aucune configuration supplémentaire ne soit nécessaire. Le mécanisme de configuration automatiquede la machine déduit sa propre adresse des informations qui lui sont communiquées par les routeurs voisins via le protocole *neighbor discovery* (ND). Ce processus ne nécessite aucune intervention de l'administrateur et présente, par rapport au distributeur d'adresses DHCP utilisé sous IPv4, l'avantage supplémentaire de supprimer le besoin de maintenir un serveur central des adresses disponibles.

Informatique nomade IPv6 permet d'associer à une interface réseau plusieurs adresses simultanées. Vous disposez ainsi, en tant qu'utilisateur d'un système, facilement et sans configuration supplémentaire, d'un accès à plusieurs réseaux différents. On peut comparer cette fonction aux utilisateurs "itinérants" des les réseaux de radiotéléphonie. Si vous êtes à l'étranger avec votre téléphone mobile, votre téléphone se connecte automatiquement sur le réseau local. Où que vous soyez, vous êtes assuré de toujours pouvoir être joint avec votre numéro de téléphone normal et vous utilisez le réseau étranger pour téléphoner comme s'il s'agissait de votre réseau habituel.

Une communication sûre Des communications sécurisées étaient certes disponibles sous IPv4, mais uniquement en faisant appel à des outils complémentaires, IPSec et donc la communication sécurisée entre deux systèmes via un tunnel traversant l'Internet non sécurisé sont désormais compris dans IPv6.

Compatibilité avec l'existant On ne peut pas envisager de façon réaliste de faire passer tout l'Internet d'IPv4 à IPv6 d'un seul coup. Il est donc important que les deux versions puissent cohabiter sur l'Internet et sur un même système. La coexistence de ces deux protocoles sur l'Internet est garantie par l'utilisation d'adresses compatibles (les adresses IPv4 se transforment facilement en adresses IPv6) et l'utilisation de différents tunnels (voir la section 22.2.3 page 429). La *double pile IP* (Dual Stack IP) permet de prendre en charge les deux protocoles sur un seul système. Chacun des deux protocoles

utilise sa propre pile réseau de manière à ce que les deux versions de protocoles ne se télescopent pas.

La multidiffusion – une offre de service sur mesure
Si avec IPv4, certains services (par exemple SMB) devaient diffuser leurs paquets à tous les membres du réseau local, on dispose d'une approche beaucoup plus fine avec IPv6. Grâce à la *multidiffusion*, on peut s'adresser à un groupe d'ordinateurs en une seule fois (c'est-à-dire pas à tous les ordinateurs simultanément en *diffusion*, ou à un seul uniquement en *envoi ciblé*). C'est l'application qui détermine les ordinateurs en question. Il existe quelques groupes de multidiffusion bien définis, tels que tous les serveurs de noms (en anglais, all name servers multicast group) ou tous les routeurs (en anglais, all routers multicast group).

22.2.2 Types et structures d'adresses

Comme nous l'avons déjà évoqué, le protocole IP utilisé jusqu'à présent présentait deux inconvénients non négligeables : on dispose de moins en moins d'adresses IP et il est de plus en plus compliqué et lourd de configurer le réseau et de gérer les tables de routage. IPv6 s'est attaqué au premier problème en étendant l'espace d'adressage à 128 bits. La solution du deuxième problème réside dans la structure d'adresse hiérarchique, dans les mécanismes conçus pour l'attribution des adresses au sein d'un réseau et dans la possibilité de *rattachement multiple* (en anglais, multi-homing, plusieurs adresses par interface avec accès à différents réseaux).

En ce qui concerne IPv6, vous devez pouvoir distinguer trois types d'adresses :

unicast (à un seul destinataire) Les adresses de ce type appartiennent à une seule interface réseau. Les paquets possédant une adresse de ce type sont livrés à un seul destinataire. Les adresses de diffusion individuelle sont utilisées pour adresser des ordinateurs individuels du réseau local ou sur l'Internet.

multicast (à plusieurs destinataires) Les adresses de ce type représentent un groupe d'interfaces. Les paquets possédant une adresse de ce type sont envoyés à tous les destinataires membres de ce groupe. Les adresses de multidiffusion sont, pour la plupart, utilisées par des services réseau particuliers, pour adresser des groupes particuliers ciblés d'ordinateurs.

anycast (pour tout les destinataires) Les adresses de ce type représentent un groupe d'interfaces. Les paquets possédant une adresse de ce type sont livrés aux membres du groupe qui est le plus "proche" de l'expéditeur au

sens du protocole de routage utilisé. Les adresses anycast sont utilisées pour permettre aux terminaux de trouver un serveur proposant un service donné dans leur domaine réseau. Tous les serveurs d'un type donné possèdent la même adresse anycast. Si le terminal demande un service, c'est le serveur le plus proche de l'hôte, selon l'évaluation du protocole de routage, qui répond. En cas d'indisponibilité de ce serveur, c'est le deuxième plus proche qui est alors utilisé, et ainsi de suite.

Une adresse IPv6 se compose de huit champs de quatre chiffres soit 16 bits chacun, représentés en écriture hexadécimale. Ils sont séparés par des deux points (`:`). On peut omettre les octets nuls de tête dans un champ, mais pas ceux qui se trouvent au milieu ou à la fin d'un champ. On peut représenter plus de quatre octets nuls qui se suivent par le signe d'omission `::`. Toutefois on ne peut utiliser qu'un seul signe d'omission dans une adresse. L'exemple 22.3 de la présente page illustre cette notation abrégée à l'aide de trois modes d'écriture équivalents pour la même adresse.

Example 22.3: *Exemple d'adresse IPv6*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                           : 10 : 1000 : 1a4
```

Chaque partie d'une adresse IPv6 a une signification particulière. Les premiers octets constituent un préfixe et indiquent le type de l'adresse. La partie centrale adresse un réseau ou n'a pas de signification particulière. La fin de l'adresse indique la partie hôte. Les masques réseau se définissent sous IPv6 par la longueur du préfixe indiquée par un `/` à la fin de l'adresse. Une adresse représentée comme dans l'exemple 22.4 de la présente page signifie que les 64 premiers bits constituent la partie réseau et les 64 derniers bits la partie réseau de l'adresse. Autrement dit, le nombre `64` indique que le masque réseau est rempli de bits 1 à partir de la gauche. Comme avec IPv4, on combine avec ET le masque réseau et l'adresse IP pour déterminer si l'ordinateur se trouve dans le même sous-réseau ou dans un autre.

Example 22.4: *Adresse IPv6 avec indication du préfixe*

```
fe80::10:1000:1a4/64
```

IPv6 reconnaît différents préfixes avec différentes significations comme montré au tableau 22.4 page ci-contre).

TAB. 22.4: *Différents préfixes IPv6*

Préfixe (hexadécimal)	Utilisation
00	Les adresses IPv4 et les adresses de compatibilité IPv4/IPv6. Il s'agit d'une adresse compatible IPv4. Un routeur approprié doit convertir le paquet IPv6 en IPv4. D'autres adresses spéciales (par exemple dispositif de bouclage loopback) possèdent également ce préfixe.
premier chiffre 2 ou 3	(en anglais, Aggregatable Global Unicast Address). Comme auparavant, vous pouvez aussi obtenir avec IPv6 des réseaux partiels. On dispose, à l'heure actuelle, des espaces d'adresses suivants : 2001::/16 (production quality address space, espace d'adressage de production), 2002::/16 (6to4 address space, espace d'adressage 6vers4).
fe80::/10	(en anglais, link-local) Les adresses avec ce préfixe ne peuvent pas être routées et ne peuvent donc être jointes qu'à l'intérieur du même sous-réseau.
fec0::/10	(en anglais, site-local) Ces adresses peuvent certes être routées, mais uniquement au sein d'une organisation. C'est pour cette raison que ces adresses correspondent aux réseaux jusqu'alors "privés" (par exemple 10.x.x.x).
ff	(en anglais, multicast) Les adresses IPv6 qui commencent par ff sont des adresses de multidiffusion.

Les adresses d'envoi ciblé comportent trois composants de base :

Topologie publique La première partie qui comprend, entre autres, l'un des préfixes présentés précédemment, sert au routage du paquet sur l'Internet public. C'est dans cette partie que les informations relatives au fournisseur d'accès ou à l'institution sont codées pour préparer l'accès au réseau.

Topologie du site La deuxième partie contient des informations de routage relatives au sous-réseau qui doit distribuer le paquet.

Identificateur de l'interface La troisième partie identifie clairement l'interface à laquelle le paquet est adressé. Cela permet ainsi d'utiliser l'adresse MAC

en tant que composant de l'adresse. Comme cette adresse est unique dans le monde entier et attribuée par le fabricant du matériel, la configuration de l'ordinateur est considérablement simplifiée. En réalité, les 64 premiers bits sont rassemblés en une unité lexicale `EUI-64`. Parallèlement, les derniers 48 bits de l'adresse MAC sont retirés et les derniers 24 bits contiennent des informations spéciales indiquant le type de l'unité lexicale. Cela permet aussi d'attribuer des unités lexicales `EUI-64` à des appareils ne disposant pas d'adresse MAC (connexions PPP et RNIS).

De cette structure de base, on déduit cinq types différents d'adresses unicast :

`::` (non précisé) Un ordinateur utilise cette adresse comme adresse source lorsqu'on initialise pour la première fois son interface — quand il ne peut pas encore déterminer son adresse par d'autres méthodes.

`::1` (bouclage) Adresse du dispositif de bouclage.

Adresse compatible IPv4 L'adresse IPv6 est tirée de l'adresse IPv4 et d'un préfixe de quatre-vingt seize bits 0 au début de l'adresse. C'est ce type d'adresses de compatibilité que l'on utilise pour les tunnels (reportez-vous à la section 22.2.3 page suivante) pour permettre aux hôtes IPv4 et IPv6 de communiquer avec d'autres se trouvant dans un résau IPv4 pur.

Adresse IPv4 avec équivalent IPv6 Ce type d'adresse indique l'adresse IPv6 d'un ordinateur IPv4 pur.

Adresses locales Il existe deux types d'adresses pour une utilisation purement locale :

link-local Ce type d'adresse est exclusivement conçu pour une utilisation dans le sous-réseau local. Les routeurs n'ont pas le droit de transmettre sur l'Internet ou à d'autres sous-réseaux les paquets dont l'adresse cible ou source est de ce type. Ces adresses se caractérisent par un préfixe spécial (`fe80::/10`) et l'identificateur d'interface de la carte réseau, dont la partie centrale est composée d'octets nuls. Les méthodes de configuration automatique utilisent ce type d'adresse pour communiquer avec des ordinateurs du même sous-réseau.

site-local Les paquets avec ce type d'adresse peuvent être routés entre différents sous-réseaux mais ne peuvent pas arriver sur l'Internet — ils doivent rester dans le réseau privé de l'organisation. Ces adresses sont utilisées pour les intranets et sont équivalentes des adresses privées d'IPv4. Ces adresses comportent un préfixe particulier (`fec0::/10`),l'identificateur de l'interface et un champ de 16 bits dans

lequel l'identificateur du sous-réseau est codé. Le reste est à nouveau comblé par des octets nuls.

L'attribution de plusieurs adresses IP à une interface réseau est une nouveauté complète d'IPv6 et présente l'avantage de pouvoir accéder à plusieurs réseaux par le biais de la même interface. Un de ces réseaux peut être configuré complètement automatiquement à l'aide de l'adresse MAC et d'un préfixe connu. Tous les ordinateurs du réseau local sont alors accessibles dès que IPv6 est activé (avec l'adresse link-local). Comme l'adresse MAC fait partie de l'adresse IP, toutes les adresses IP utilisées dans le monde sont uniques. Seules les parties définissant la *topologie du site* et la *topologie publique* peuvent varier selon le réseau dans lequel l'ordinateur fonctionne actuellement.

Si un ordinateur se ″déplace“ entre plusieurs réseaux, il a besoin d'au moins deux adresses. L'une, son ″adresse personnelle“ (home address), contient outre l'identificateur de l'interface, des informations relatives à son réseau d'exploitation d'origine et le préfixe correspondant. L'″adresse personnelle“ est statique et n'est pas modifiée. Tous les paquets adressés à cet ordinateur lui sont transmis, qu'il se trouve sur son propre réseau ou sur un réseau étranger. La distribution sur le réseau étranger est prise en charge par des nouveautés essentielles du protocole IPv6, notamment l'″auto-configuration sans état“ et la ″découverte de voisins“. L'ordinateur mobile possède, outre son ″adresse personnelle“, une ou plusieurs autres adresses qui se trouvent sur les réseaux étrangers dans lequel il se déplace. Ces adresses sont des adresses ″aux bons soins de“ (care-of address). Il doit y avoir dans le réseau d'origine de l'ordinateur mobile une instance qui ″redirige“ sur son ″adresse personnelle“ lorsqu'il se trouve dans un autre réseau. Cette fonction est assurée, dans un scénario IPv6 par le ″Home Agent“. Ce dernier distribue tous les paquets adressés à l'adresse personnelle de l'ordinateur mobile via un tunnel. Les paquets dont l'adresse de destination est l'adresse ″aux bons soins de“ peuvent ainsi être distribués directement.

22.2.3 Coexistence de IPv4 et de IPv6

Le passage d'IPv4 à IPv6 de tous les ordinateurs présents sur l'Internet ne se fera pas d'un coup. L'ancien et le nouveau protocole devraient encore cohabiter pendant un certain temps. La coexistence, sur un ordinateur, est assurée par la *double pile*, mais reste encore la question de la communication entre les ordinateurs IPv6 et IPv4 et comment IPv6 doit être transporté sur les réseaux IPv4 encore majoritaires. Les tunnels et l'utilisation d'adresses de compatibilité (reportez-vous à la section 22.2.2 page 425) font partie des meilleures solutions.

Les îlots IPv6 dans le réseau IPv4 mondial échangent leurs données par l'intermédiaire de tunnels. Dans le cadre des tunnels, les paquets IPv6 sont encapsulés dans des paquets IPv4 pour pouvoir être transportés via un réseau IPv4 pur. Un tunnel est une connexion entre deux points terminaux IPv4. Il convient donc d'indiquer l'adresse IPv6 cible (ou le préfixe correspondant) à laquelle les paquets IPv6 déguisés doivent être envoyés et l'adresse IPv4 distante qui doit recevoir les paquets du tunnel. Dans les cas les plus simples, les administrateurs configurent ce type de tunnel entre leurs réseaux *manuellement* et après accord. On parle alors de tunnel *statique*.

Toutefois, la configuration et la maintenance de tunnels statiques est souvent trop laborieuse pour être utilisée au quotidien. C'est pour cette raison que IPv6 offre trois différentes méthodes pour avoir des tunnels *dynamique*.

6sur4 (6over4) Les paquets IPv6 sont automatiquement encapsulés dans des paquets IPv4 et envoyés via un réseau IPv4 dans lequel la multidiffusion est activée. Pour IPv6, la totalité du réseau (d'un internet) apparaît comme un seul immense réseau local. Cela permet toujours de déterminer automatiquement le point terminal IPv4 du tunnel. Un inconvénient de cette méthode réside le fait qu'elle monte mal en charge et dans le fait que la multidiffusion IP est loin d'être disponible sur la totalité de l'Internet. Cette solution n'est donc adaptée que pour les réseaux plus réduits de sociétés ou d'institutions qui permettent de faire de la multidiffusion IP. Le RFC correspondant est le RFC 2529.

6vers4 (6to4) Cette méthode génère automatiquement des adresses IPv4 à partir d'adresses IPv6. Les îlots IPv6 peuvent ainsi communiquer les uns avec les autres via un réseau IPv4. Il demeure cependant quelques problèmes pour ce qui concerne la communication entre les îlots IPv6 et l'Internet. Le RFC correspondant est le RFC 3056.

IPv6 Tunnel Broker Cette approche prévoit des serveurs spéciaux qui définissent automatiquement des tunnels pour l'utilisateur. Le RFC correspondant est le RFC 3053.

Important

L'initiative 6Bone

Au sein de l'Internet "à l'ancienne mode", le réseau *6Bone* (`www.6bone.net`) constitue un réseau mondial réparti de sous-réseaux IPv6 connectés par des tunnels. Les programmeurs et les fournisseurs d'accès qui développent ou proposent des services IPv6 peuvent utiliser cet environnement de test pour acquérir l'expérience nécessaire avec ce nouveau protocole. Vous trouverez davantage d'informations à ce sujet sur le site Internet du projet.

Important

22.2.4 Configurer IPv6

Vous n'aurez normalement pas à faire de modification sur les postes de travail individuels pour configurer IPv6. La prise en charge d'IPv6 doit toutefois être activée. Pour cela, saisissez `modprobe ipv6` en tant que `root`.

Grâce au principe d'autoconfiguration de IPv6, la carte réseau se voit attribuer une adresse dans le réseau *link-local*. Normalement, une station de travail ne gère pas les tables de routage. Les routeurs du réseau peuvent être interrogés par la station de travail avec le *protocole d'annonce des routeurs* (RAP, Router Advertisement Protocol) pour connaître le préfixe et la passerelle à mettre en place. On peut utiliser le programme radvd pour paramétrer un routeur IPv6. Ce programme informe les stations de travail à propos du préfixe et des routeurs à utiliser pour les adresses IPv6. Vous pouvez aussi utiliser zebra pour configurer automatiquement les adresses et le routage.

Consultez la page de manuel de ifup (`man ifup`) pour obtenir des informations à propos de la mise en place des différents types de tunnels grâce aux fichiers `/etc/sysconfig/network`.

22.2.5 Documentation et liens supplémentaires au sujet d'IPv6

La présentation ci-dessus ne peut et ne se veut en aucun cas une introduction complète au sujet très complexe qu'est IPv6. Pour une approche plus approfondie d'IPv6, vous pouvez consulter la documentation en ligne et les ouvrages suivants :

`http://www.ngnet.it/e/cosa-ipv6.php`
: Série d'articles avec de très bonnes descriptions sur les principes fondamentaux d'IPv6. Particulièrement appropriés pour une première approche de ce sujet.

`http://www.bieringer.de/linux/IPv6/`
: Linux-IPv6-HOWTO et nombreux liens.

`http://www.6bone.net/` Se connecter à IPv6 par un tunnel.

`http://www.ipv6.org/` Tout sur IPv6.

RFC 2640 Le RFC d'introduction au sujet d'IPv6.

IPv6 Essentials Présentation en anglais d'IPv6. Hagen, Silvia : *IPv6 Essentials*. O'Reilly & Associates, 2002. - (ISBN 0-596-00125-8).Voir aussi en français : Cizault, Gisèle :*IPv6, théorie et pratique*. O'Reilly & Associates, 2002. - (ISBN : 2-84177-139-3).

22.3 Résolution de noms

Le DNS permet d'associer une adresse IP à un ou plusieurs noms et d'associer un nom à une adresse IP. Sous Linux, cette conversion est généralement assurée par un logiciel spécial appelé bind. L'ordinateur qui réalise ensuite cette conversion s'appelle le *serveur de noms*. Les noms constituent alors un système hiérarchique dans lequel les composants individuels du nom sont séparés par des points. La hiérarchie de noms est toutefois indépendante de la hiérarchie des adresses IP décrite précédemment.

Examinons un instant un nom complet, par exemple `laurent.suse.de` écrit au format `nomhôte.domaine`. Un nom complet, appelé "nom pleinement qualifié" (Fully Qualified Domain Name ou en abrégé *FQDN*) est composé d'un nom d'hôte et d'un nom de domaine (`suse.de`). Ce dernier contient aussi le *domaine de premier niveau* ou TLD (Top Level Domain soit, en l'occurrence, `de`).

Pour des raisons historiques, l'attribution des TLD est quelque peu déconcertante. Traditionnellement, on utilise aux États-Unis des TLD classiques de trois lettres. Dans le reste du monde, on utilise les désignations de pays ISO composées de deux lettres. Des TLD plus longs supplémentaires ont été introduits en 2000 pour représenter certaines activités (par exemple `.info`, `.name`, `.museum`).

Aux débuts de l'Internet (avant 1990), le fichier `/etc/hosts` contenait tous les noms des ordinateurs présents sur l'Internet. Ceci s'est révélé rapidement impraticable en raison de la croissance extrêmement rapide du nombre d'ordinateurs

connectés à l'Internet. C'est pour cette raison que l'on a mis en place une base de données décentralisée qui peut enregistrer les noms d'ordinateurs de manière distribuée. Cette base de données, similaire à un serveur de noms,ne contient pas toutes les données de tous les ordinateurs présents sur l'Internet, mais peut faire suivre à d'autres serveurs de noms des demandes qui lui sont adressées.

Tout en haut de la hiérarchie, on trouve les "serveurs de noms racine" Root-Nameserver, qui gèrent les domaines de premier niveau. Les serveurs de noms racine sont gérés par le Network Information Center (*NIC*). Le serveur de noms racine connaît les serveurs de noms responsables pour un domaine de premier niveau. Pour plus d'informations sur le NIC des domaines de premier niveau, consultez `http://www.internic.net`.

Le DNS peut faire bien plus que simplement résoudre les noms de machines. Ainsi, le serveur de noms saitaussi quel ordinateur prend en charge les messages électroniques pour tout un domaine — le serveur de messagerie *mail exchanger (MX)*.

Pour que votre ordinateur puisse convertir un nom en adresse IP, il doit au moins connaître l'adresse IP d'un serveur de noms. YaST vous permet de configurer facilement un serveur de noms. Si vous utilisez une connexion par modem, il est possible que vous n'ayiez pas à configurer de serveur de nom manuellement. Vous trouverez une description de la configuration de l'accès au serveur de noms sous SUSE LINUX dans le chapitre 24 page 463.

Le protocole `whois` est intimement lié au DNS. Vous pouvez utiliser le programme du même nom, whois, pour retrouver rapidement le responsable d'un domaine donné.

22.4 Configurer une connexion réseau avec YaST

L'ordinateur doit disposer d'une carte réseau prise en charge. Celle-ci a généralement déjà été reconnue lors de l'installation et le pilote approprié mis en place. Si votre carte a été correctement installée avec le bon pilote, saisissez la commande `ip address list eth0`. Elle donnera une liste d'informations sur le périphérique réseau `eth0` ou affichera un message d'erreur.

Si la prise en charge du noyau pour la carte réseau est mise en œuvre sous forme de module, ce qui est normalement le cas pour le noyau SUSE le nom du module

doit être saisi dans `/etc/sysconfig/hardware/hwcfg-*`. Si rien n'est indiqué ici, `hotplug` sélectionne automatiquement un pilote. Quel que soit le type de carte réseau (que l'on peut brancher à chaud ou intégrée), `hotplug` affecte un pilote.

22.4.1 Configurer une carte réseau avec YaST

Après le démarrage du module de YaST, vous obtenez un résumé de la configuration réseau. Dans la partie supérieure de la boîte de dialogue, toutes les cartes réseau à configurer sont affichées. Si votre carte a été détectée correctement à l'amorçage du système, elle sera mentionnée ici. Les périphériques non reconnus apparaissent comme 'Autre (non détecté)'. Dans la partie inférieure de la fenêtre d'affichage, les périphériques déjà configurés sont affichés ainsi que leurs type et adresse réseau. Vous pouvez maintenant configurer les nouvelles cartes réseau ou changer une configuration déjà existante.

Configuration manuelle d'une carte réseau

La configuration d'une carte réseau qui n'a pas été détectée (une carte répertoriée comme 'Autre') inclut les éléments suivants :

Configuration du réseau Définissez le type de périphérique de l'interface et le nom de la configuration. Sélectionnez le type de périphérique parmi les options proposées. Spécifiez un nom de configuration suivant vos besoins. Les réglages par défaut conviennent d'ordinaire et peuvent être acceptés. Vous trouverez des informations sur les conventions de nommage concernant les noms de fichiers de configuration dans la page de manuel de `getcfg`.

Module du noyau 'Nom de la configuration du matériel' indique le nom du fichier `/etc/sysconfig/hardware/hwcfg-*` contenant les réglages matériels de votre carte réseau, le nom du module du noyau approprié. YaST propose dans la plupart des cas des noms judicieux pour les périphériques PCMCIA et USB. Pour tout autre matériel, `0` n'a habituellement de sens que si la carte est configurée avec `hwcfg-static-0`.

Si la carte réseau est un périphérique PCMCIA ou USB, activez les cases à cocher correspondantes et quittez la boîte de dialogue en cliquant sur 'Suivant'. Si ce n'est pas le cas, choisissez le modèle de votre carte réseau à l'aide du bouton 'Sélectionner dans la liste'. YaST choisira alors automatiquement le module de noyau adéquat. Cliquez sur 'Suivant' pour quitter cette boîte de dialogue.

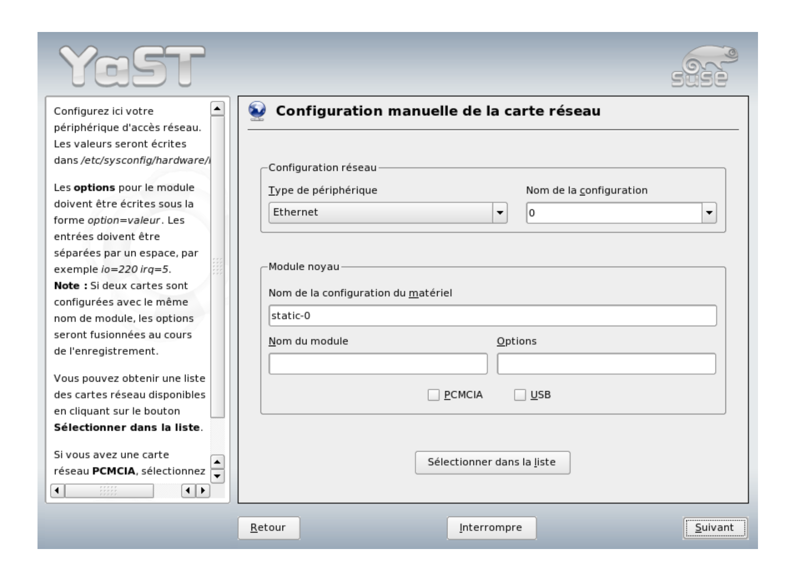


FIG. 22.3: *Configuration de la carte réseau*

Configuration de l'adresse réseau

Définissez le type de périphérique de l'interface et le nom de la configuration. Sélectionnez le type de périphérique parmi les options proposées. Spécifiez un nom de configuration suivant vos besoins. Les réglages par défaut conviennent d'ordinaire et peuvent être acceptés. Vous trouverez des informations sur les conventions de nommage concernant les noms de fichiers de configuration dans la page de manuel de `getcfg`.

Si vous avez choisi 'sans fil' comme type de périphérique pour l'interface, configurez le mode de fonctionnement, le nom du réseau (ESSID) et le chiffrement dans la boîte de dialogue suivante, 'Configuration périphériques sans fil'. Cliquez sur 'OK' pour achever la configuration de votre carte. Une description détaillée de la configuration des cartes WLAN se trouve dans la section 17.1.3 page 352. Pour tous les autres types d'interfaces, poursuivez avec la configuration de l'adresse réseau :

'Affectation dynamique d'adresses (via DHCP)'
Si vous disposez d'un serveur DHCP dans votre réseau, vous pouvez en obtenir automatiquement les données de configuration pour votre carte

réseau. Activez également l'affectation d'adresses IP via DHCP si votre fournisseur d'accès à l'ADSL n'attribue pas d'adresse IP statique à votre système. Pour accéder à la configuration du client DHCP, utilisez l'option 'Options du client DHCP'. Ici vous pouvez indiquer si le serveur DHCP doit toujours répondre à une diffusion générale (broadcast). En outre, vous avez la possibilité d'indiquer un identificateur. Par défaut, l'ordinateur identifie la carte réseau au moyen de l'adresse matérielle. Si vous utilisez plusieurs machines virtuelles qui font appel à la même carte réseau, vous pouvez les différencier à l'aide d'identificateurs différents.

'Réglage d'une l'adresse statique' Si vous disposez d'une adresse IP, cochez la case correspondante. Saisissez ici votre adresse IP et le masque sous-réseau qui convient à votre réseau. La configuration par défaut du masque sous-réseau est suffisante pour un réseau domestique ordinaire.

Quittez cette boîte de dialogue en cliquant sur 'Suivant' ou continuez en configurant le nom d'hôte, le serveur de noms et les détails de routage (voir la page 64 et la page 66).

'Avancé' vous permet d'indiquer des réglages plus complexes. Dans 'Paramètres détaillés', utilisez 'Contrôlé par l'utilisateur' pour déléguer le contrôle de la carte réseau depuis l'administrateur (le `root`) à l'utilisateur normal. Dans un contexte d'informatique nomade, ceci permet à l'utilisateur d'adapter les connexions réseau changeantes d'une manière plus flexible, car il peut contrôler l'activation ou la désactivation de l'interface. La MTU (Maximum Transmission Unit - Unité de Transmission Maximale) et le type d''Activation du périphérique' sont également réglés dans cette boîte de dialogue.

22.4.2 Modem

Dans le centre de contrôle de YaST, vous trouverez la configuration du modem dans 'Périphériques réseau'. Si la détection automatique n'aboutit pas, choisissez la configuration manuelle. Dans la boîte de dialogue qui s'ouvre, indiquez l'interface dans 'Modem'.

Si votre ligne passe par un central téléphonique privé, vous devrez éventuellement indiquer un préfixe (normalement zéro ; vous pouvez vous en assurer en consultant le mode d'emploi de votre central téléphonique) pour passer des appels extérieurs. Choisissez en outre entre la numérotation par tonalité et la numérotation par impulsions. Vous pouvez aussi décider si la sortie son du modem doit être activée et si vous désirez attendre la tonalité. Vous ne devriez pas utiliser cette dernière option si votre modem est relié à un autocommutateur (PABX).

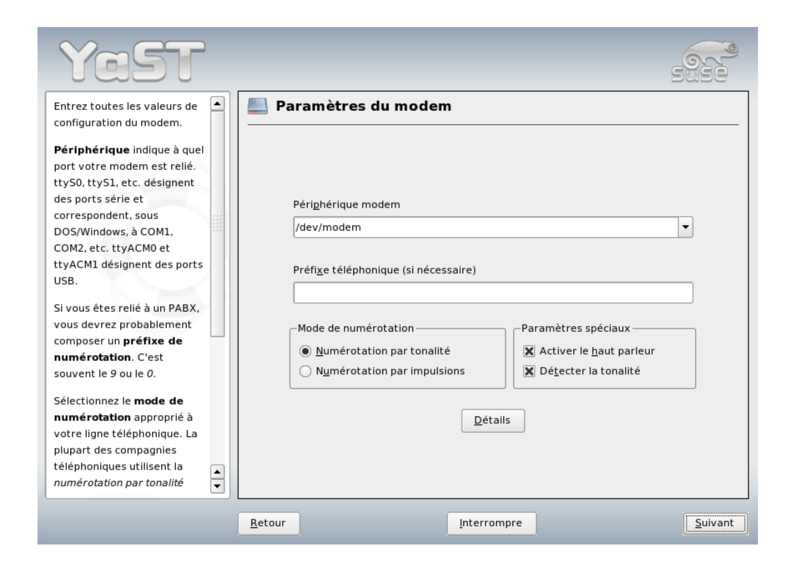


FIG. 22.4: *Configurer un modem*

Dans 'Détails', définissez le débit en bauds et les chaînes d'initialisation du modem. Ces réglages ne changent que si votre modem n'a pas été détecté automatiquement ou s'il exige des réglages spéciaux pour que la transmission des données fonctionne. C'est notamment le cas pour les adaptateurs terminaux RNIS. Quittez cette boîte de dialogue en cliquant sur 'OK'. Pour déléguer le contrôle du modem à l'utilisateur normal sans droits root, cochez 'Contrôlé par l'utilisateur'. De cette manière, l'utilisateur sans droits d'administrateur peut activer ou désactiver une interface. Dans 'Expression régulière du préfixe de numérotation' indiquez une expression régulière. Dans KInternet, l'option 'Préfixe de numérotation' qui peut être modifiée par l'utilisateur normal doit correspondre à cette expression régulière. Si ce champ est laissé vide, l'utilisateur ne peut pas définir un 'Préfixe de numération' sans droits d'administrateur.

Dans la boîte de dialogue suivante, choisissez le FAI (Fournisseur d'Accès à Internet). Pour choisir dans une liste prédéfinie de FAI opérant dans votre pays, cliquez sur 'Pays'. Autrement, cliquez sur 'Nouveau' pour ouvrir une boîte de dialogue dans laquelle vous saisirez les paramètres de votre FAI. Ceux-ci comprennent un nom pour la connexion sortante et le FAI, ainsi que le nom d'utilisateur et le mot de passe que votre FAI vous a attribués. Cochez la case 'Toujours

demander' si vous souhaitez que le mot de passe vous soit demandé à chaque connexion.

Dans la dernière boîte de dialogue, indiquez les options de connexion supplémentaires :

'Connexion à la demande' Si vous souhaitez utiliser une connexion à la demande, indiquez au moins un serveur de noms.

'Modifier le DNS après connexion' Cette case est cochée par défaut, ce qui a pour effet de mettre à jour l'adresse du serveur de noms chaque fois que vous vous connectez à l'Internet. Toutefois, si vous activez 'Connexion à la demande', décochez cette case et définissez une adresse de serveur de noms fixe.

'Retrouver automatiquement le DNS'
Si le fournisseur ne transmet pas son serveur de noms de domaine après connexion, décochez cette option et saisissez les données concernant le serveur de noms manuellement.

'Mode stupide' Cette option est cochée par défaut. Grâce à elle, les invites de saisie qu'envoie le serveur du FAI sont ignorées pour les empêcher d'interférer avec le processus de connexion.

'Activer le pare-feu' En cochant cette option, vous activez le pare-feu SUSE, ce qui vous protège des attaques extérieures pour la durée de votre connexion Internet.

'Délai d'inactivité (secondes)' Vous pouvez fixer le délai après lequel la communication sera automatiquement coupée si aucun échange d'informations n'a lieu.

'Détails IP' Ce bouton permet d'ouvrir la boîte de dialogue de configuration de l'adresse. Si votre fournisseur d'accès ne vous a attribué aucune adresse IP dynamique, décochez la case 'Adresse IP dynamique' et saisissez l'adresse IP locale de votre ordinateur et l'adresse IP distante. Vous pouvez obtenir ces adresses auprès de votre fournisseur d'accès. Laissez la configuration de 'Route par défaut' activée et quittez la boîte de dialogue en cliquant sur 'OK'.

Cliquez sur 'Suivant' pour retourner à la boîte de dialogue d'aperçu dans laquelle la configuration est affichée. Quittez la configuration avec 'Terminer'.

22.4.3 RNIS

Utilisez ce module pour configurer une ou plusieurs cartes RNIS dans votre système. Si YaST n'a pas détecté votre carte RNIS, choisissez-la manuellement. De

multiples interfaces sont possibles, mais plusieurs FAI peuvent être configurés pour une interface. Les boîtes de dialogue suivantes servent à définir les options RNIS nécessaires pour le fonctionnement correct de la carte.

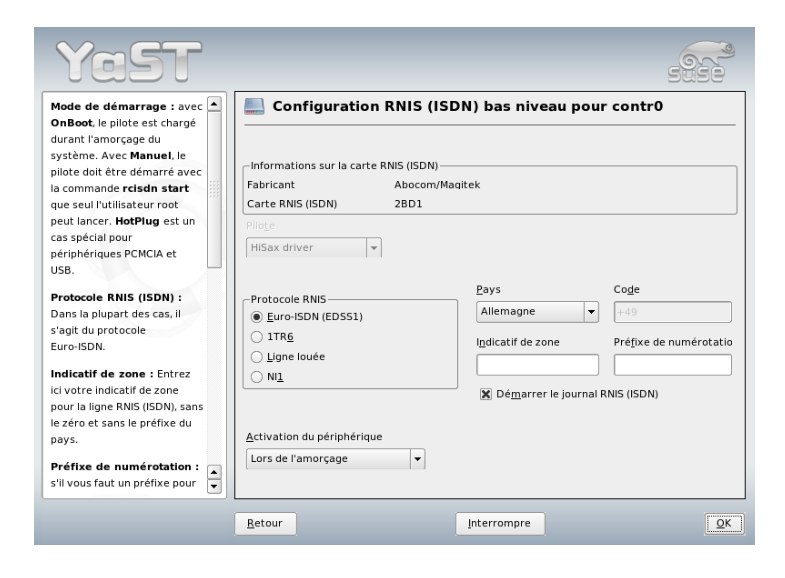


FIG. 22.5: *Configuration du RNIS*

Dans la boîte de dialogue suivante, illustrée sur la figure 22.5 de la présente page), sélectionnez le protocole à utiliser. Par défaut, il s'agit de 'Euro-ISDN (EDSS1)', mais pour les systèmes téléphoniques anciens ou pour les grandes installations, choisissez '1TR6'. Si vous êtes aux États-Unis, choisissez 'NI1'. Sélectionnez votre pays dans le champ approprié. Le code du pays correspondant apparaît alors dans le champ de saisie à côté. Pour finir, saisissez votre 'Préfixe régional' et le préfixe de numérotation (si nécessaire).

'Mode de démarrage' définit comment démarrer l'interface RNIS : 'OnBoot' entraîne l'initialisation du pilote RNIS à chaque amorçage du système. 'Manuel' suppose que vous chargiez le pilote RNIS manuellement en tant que super-utilisateur avec la commande `rcisdn start`. L'option 'Hotplug', utilisée pour les périphériques PCMCIA ou USB, charge le pilote après que le périphérique soit branché. Quand vous en avez fini avec tous ces réglages, cliquez sur 'OK'.

Dans la boîte de dialogue suivante, spécifiez le type d'interface de votre carte RNIS et ajoutez les FAI à une interface existante. Les interfaces peuvent être

soit du type `SyncPPP`, soit `RawIP`, mais la plupart des FAI opèrent en mode `SyncPPP`, décrit ci-dessous.

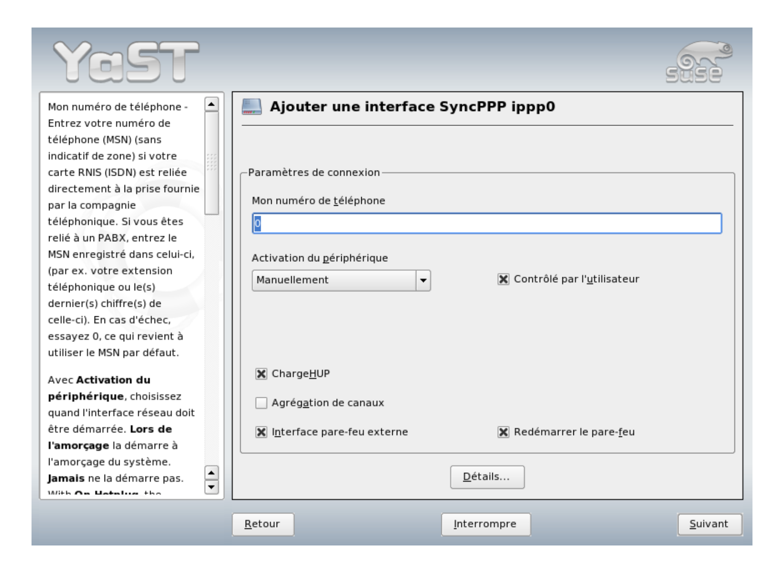


FIG. 22.6: *Configuration des interfaces RNIS*

Le numéro à saisir pour 'Mon numéro de téléphone' dépend de votre propre installation :

La carte RNIS est branchée directement à la prise téléphonique
RNIS vous offre normalement trois numéros de téléphone par connexion (MSN, Multiple Subscriber Number) qui, sur demande, peuvent être augmentés à dix numéros. Vous devez affecter un des numéros MSN à votre carte RNIS (à indiquer sans préfixe). Si vous faites une erreur, cela devrait malgré tout fonctionner, car votre compagnie téléphonique devrait dans ce cas remplacer le numéro erroné par le premier MSN attribué à votre raccordement RNIS.

La carte RNIS est reliée à un central téléphonique
Ici aussi, la configuration peut dépendre de l'équipement installé :

1. Pour l'utilisation privée : le protocole de l'autocommutateur (PABX) pour les raccordements internes est Euro-ISDN/EDSS1 (c'est généra-

lement le cas pour les petites installations à usage privé). Ces installations sont dotées d'un bus S0 interne et utilisent des numéros internes pour les appareils connectés.

Utilisez un des numéros internes pour indiquer le MSN. L'un ou l'autre des numéros devrait fonctionner à condition que l'accès vers l'extérieur soit disponible pour ce MSN. Mais en cas de besoin, un simple zéro devrait aussi pouvoir fonctionner. Vous trouverez des informations plus précises dans la documentation qui accompagne votre PABX.

2. Pour un usage professionnel : le protocole de l'autocommutateur (PABX) pour les raccordements internes est 1TR6 (ceci n'est cependant le cas que pour les grandes installations en entreprise). Le MSN est ici remplacé par l'EAZ (en allemand, Endgeräte-Auswahl-Ziffer = numéro de sélection de l'appareil terminal). Lors de la configuration sous Linux, seul le dernier chiffre de l'EAZ doit en principe être spécifié. En dernière extrêmité, essayez tous les chiffres de 1 à 9.

Cochez la case correspondante si vous souhaitez une déconnexion automatique avant le début de la prochaine unité de taxation 'ChargeHUP'. Notez cependant que ce mécanisme ne fonctionne pas encore avec tous les FAI. Pour bénéficier d'une 'Agrégation de canaux' (Multilink PPP), cochez la case correspondante. Pour finir, vous pouvez activer SuSEfirewall2 en cochant la case 'Activer firewall'. Pour permettre à l'utilisateur normal sans droits d'administrateur d'activer ou de désactiver l'interface, cochez la case 'Contrôlé par l'utilisateur'.

Un clic sur 'Détails...' ouvre une boîte de dialogue permettant de mettre en œuvre des schémas de connexion, ce qui n'a aucun intérêt pour les utilisateurs privés. Quittez cette boîte de dialogue en cliquant sur 'Suivant'.

Dans la boîte de dialogue suivante, indiquez les paramètres relatifs à l'affectation des adresses IP. Si votre fournisseur d'accès ne vous a affecté aucune adresse IP statique, choisissez 'Adresse IP dynamique'. Dans le cas contraire, saisissez dans les champs correspondants et selon les instructions de votre fournisseur d'accès, l'adresse IP locale de votre ordinateur ainsi que l'adresse IP distante. Si vous souhaitez utiliser cette interface en tant que route par défaut, cochez la case 'Route par défaut'. Notez que vous ne pouvez utiliser qu'une interface comme route par défaut par système. Quittez cette boîte de dialogue en cliquant sur 'Suivant'.

La boîte de dialogue suivante vous permet d'indiquer votre pays et de choisir un fournisseur d'accès. Les FAI de la liste sont tous du type sans abonnement. Si votre fournisseur d'accès n'est pas dans la liste, cliquez sur 'Nouveau'. La boîte de dialogue 'Paramètres du fournisseur' apparaît, dans laquelle vous saisissez

tous les détails concernant votre FAI. Les chiffres qui constituent le numéro de téléphone ne doivent pas être séparés par des virgules ou des espaces. Saisissez pour finir votre nom d'utilisateur et le mot de passe tels que votre FAI vous les a communiqués. Lorsque vous avez terminé, cliquez sur 'Suivant'.

Pour utiliser l'option 'Connexion à la demande' sur une station de travail autonome, précisez également le serveur de noms (serveur DNS). La plupart des fournisseurs d'accès gèrent le DNS dynamique, ce qui signifie que l'adresse IP d'un serveur de noms est transmise par le FAI chaque fois que vous vous connectez. Pour une station de travail isolée, cependant, vous devez encore fournir une adresse de remplacement comme `192.168.22.99`. Si votre FAI ne prend pas en charge le DNS dynamique, indiquez les adresses IP du serveur de noms de votre FAI. Si vous le souhaitez, fixez un temps imparti pour la connexion—la période d'inactivité du réseau (en secondes) après laquelle la connexion devra être automatiquement désactivée. Confirmez vos réglages par 'Suivant'. YaST affiche un résumé des interfaces configurées. Pour rendre tous ces réglages actifs, cliquez sur 'Terminer'.

22.4.4 Modem câble

Dans certains pays (Autriche, États-Unis), l'accès à Internet par câble télévision est très répandu. L'abonné reçoit de l'opérateur de réseau câblé un modem relié d'une part au câble TV et d'autre part à une carte réseau dans l'ordinateur au moyen d'un câble 10Base-T (paire torsadée). Ce modem représente alors pour la machine une ligne permanente avec une adresse IP fixe.

Après avoir configuré votre fournisseur d'accès, choisissez entre 'Assignation dynamique d'adresses (via DHCP)' ou 'Assignation statique d'adresses', en fonction des informations que vous avez obtenues de votre fournisseur d'accès Internet. La plupart des fournisseurs d'accès utilisent aujourd'hui DHCP. Une adresse IP statique fait souvent partie d'une offre réservée aux entreprises.

22.4.5 ADSL

Pour configurer une connexion ADSL, utilisez le module de YaST 'DSL' dans la rubrique 'Périphériques réseau'. Plusieurs boîtes de dialogue vous permettent de saisir les paramètres d'accès à Internet via ADSL. Avec YaST, vous pouvez configurer des connexions ADSL qui utilisent les protocoles suivants :

- PPP sur Ethernet (PPPoE)
- PPP sur ATM (PPPoATM)

- CAPI pour ADSL (Cartes Fritz)
- Protocole de tunnel point à point (PPTP) — Autriche

La configuration d'une connexion ADSL basée sur PPPoE ou PPTP exige une configuration correcte de la carte réseau. Si vous ne l'avez pas encore fait, configurez la carte en cliquant sur 'Configurer les cartes réseau' (voir la section 22.4.1 page 434). Dans le cas d'une liaison ADSL, les adresses peuvent être affectées automatiquement mais non via DHCP. C'est pourquoi vous ne devrez pas utiliser l'option 'Assignation automatique d'adresses (via DHCP)'. À la place, saisissez une adresse statique fictive pour l'interface, telle que `192.168.22.1`. Dans 'Masque sous-réseau', saisissez `255.255.255.0`. Si vous configurez un système monoposte, laissez 'Passerelle par défaut' vide.

Astuce

Les valeurs des champs 'Adresse IP' et 'Masque sous-réseau' ne sont que des valeurs fictives. Elles ne sont nécessaires que pour initialiser la carte réseau et ne représentent pas la liaison ADSL en tant que telle.

Astuce

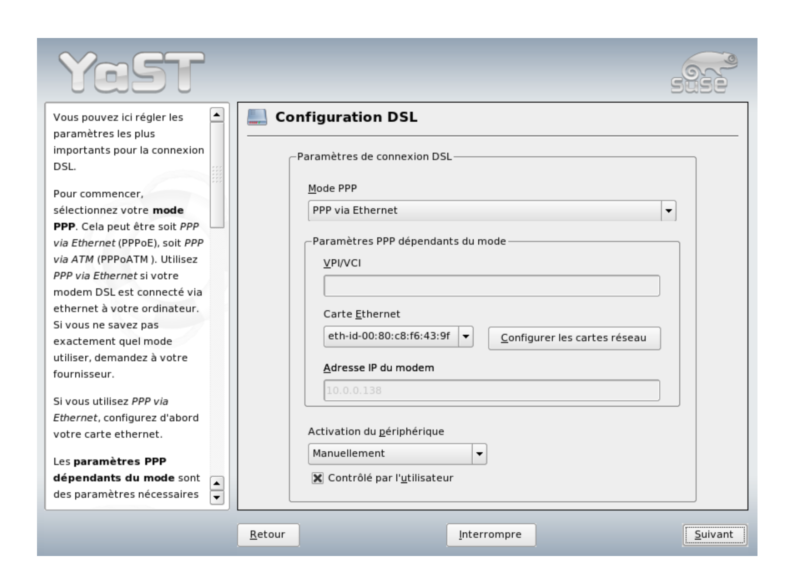


FIG. 22.7: *Configuration DSL*

Pour commencer la configuration ADSL (voir la figure 22.7 page précédente), choisissez d'abord le mode PPP et la carte Ethernet à laquelle le modem ADSL est connecté (il s'agit en général de `eth0`). Dans la zone de liste modifiable 'Activation du périphérique', spécifiez ensuite si la connexion ADSL devra être établie au cours du processus d'amorçage. Cliquez sur 'Contrôlé par l'utilisateur' pour autoriser l'utilisateur normal sans droits d'administrateur à activer ou désactiver l'interface au travers de KInternet. La boîte de dialogue vous permet également de sélectionner votre pays et de faire votre choix parmi un certain nombre de FAI qui y opèrent. Les détails des boîtes de dialogue suivantes dépendent des options définies jusqu'ici. C'est pourquoi ils ne sont que brièvement mentionnés dans les paragraphes suivants. Pour en savoir plus sur les options disponibles, lisez l'aide détaillée disponible dans les boîtes de dialogue.

Pour utiliser l'option 'Connexion à la demande' sur une station de travail autonome, spécifiez également le serveur de noms (serveur DNS). La plupart des fournisseurs d'accès gèrent le DNS dynamique—l'adresse IP d'un serveur de noms est transmise par le FAI chaque fois que vous vous connectez. Pour une station de travail isolée, cependant, indiquez une adresse de remplacement comme `192.168.22.99`. Si votre FAI ne prend pas en charge le DNS dynamique, indiquez l'adresse IP du serveur de noms fournis par votre FAI.

La liste déroulante 'Temps d'inactivité (secondes)' vous permet de définir un délai d'inactivité après lequel la connexion sera automatiquement désactivée. Une valeur raisonnable est comprise entre soixante et trois cents secondes. Si l'option 'Connexion à la demande' est désactivée, il peut être utile de définir le délai à zéro pour empêcher le raccrochage automatique.

La configuration de T-DSL est très similaire à celle de l'ADSL. Sélectionnez simplement 'T-Online' en tant que FAI, et YaST ouvre la boîte de dialogue de configuration T-DSL. Dans cette boîte de dialogue, saisissez quelques informations supplémentaires requises pour T-DSL— l'identificateur de ligne, le numéro T-Online, le code d'utilisateur et votre mot de passe. Toutes ces informations doivent être contenues sur le document que vous recevez après vous être abonné à T-DSL.

22.5 Configurer une connexion réseau manuellement

Les logiciels réseau ne devraient être configurés manuellement qu'en second recours. Nous recommandons d'utiliser YaST. Toutefois, connaître les mécanismes sous-jacents de la configuration réseau facilitera votre travail avec YaST.

Toutes les cartes réseau — qu'elles soient intégrées ou qu'il s'agisse d'un périphérique branché à chaud (PCMCIA, USB et certaines cartes PCI) — seront reconnues et installées par le biais de hotplug. Une carte réseau est vue par le système de deux manières. Elle est d'une part considérée comme un périphérique physique et d'autre part comme une interface. Le branchement ou la détection du périphérique entraîne un événement de branchement à chaud (hotplug event). Cet événement entraîne alors l'initialisation du périphérique par le biais du script `/sbin/hwup`. Lorsque une carte réseau est initialisée en tant que nouvelle interface réseau, le noyau déclenche un événement supplémentaire. Cela entraîne l'installation de l'interface par le biais de `/sbin/ifup`.

Le noyau associe les noms d'interfaces suivant l'ordre de leur enregistrement. L'ordre d'initialisation est déterminant pour l'attribution des noms. Si, en présence de plusieurs cartes réseau, l'une d'elles tombe en panne, la numérotation de toutes celles qui sont initialisées ensuite est décalée. Pour les cartes qui peuvent réellement être branchées à chaud, le plus important est l'ordre dans lequel les périphériques sont associés.

Pour obtenir une configuration flexible, la configuration des périphériques (matériel) et celle des interfaces sont séparées et l'association des configurations à leurs périphériques et interfaces respectifs ne dépend plus des noms des interfaces. La configuration des périphériques se trouve dans `/etc/sysconfig/hardware/hwcfg-*` tandis que la configuration des interfaces se trouve dans `/etc/sysconfig/network/ifcfg-*`. Les noms des fichiers de configuration sont choisis de manière à ce qu'ils décrivent leurs périphériques et interfaces respectifs. Comme l'association précédente entre les pilotes et les noms d'interface supposait que les noms d'interface soient statiques, cette association ne peut plus avoir lieu dans `/etc/modprobe.conf`. Avec le nouveau principe de fonctionnement, les déclarations d'alias dans ce fichier pourraient provoquer des effets secondaires indésirables.

Les noms des configurations — c'est à dire tout ce qui suit `hwcfg-` ou `ifcfg` — peuvent décrire les périphériques au moyen de l'emplacement dans lequel il est monté, d'un identifiant propre au périphérique ou du nom de l'interface. Par exemple, pour une carte PCI il pourrait s'agir de `bus-pci-0000:02:01.0` (emplacement PCI) ou de `vpid-0x8086-0x1014-0x0549` (identifiant du fabricant et du produit). Le nom de l'interface correspondante pourrait être également `bus-pci-0000:02:01.0` ou encore `wlan-id-00:05:4e:42:31:7a` (adresse MAC).

Si on ne veut pas associer une configuration à une carte donnée mais plutôt à une carte d'un type donné (une seule carte de ce type étant branchée à la fois), on choisit un nom de configuration moins particulier. On utilise alors par exemple

bus-pcmcia pour toutes les cartes PCMCIA. D'autre part, les noms peuvent aussi être limités par l'utilisation du type d'interface. Ainsi, wlan-bus-usb concernera toutes les cartes WLAN branchées à un port USB.

La configuration utilisée est toujours celle qui décrit le mieux l'interface ou le périphérique qui fournit l'interface. La meilleure configuration sera recherchée par /sbin/getcfg. getcfg fournit toutes les informations que l'on peut utiliser pour décrire un périphérique. Les détails concernant les noms de configuration se trouvent dans la page de manuel de getcfg.

Avec la méthode décrite, une interface réseau est configurée avec la configuration correcte, même lorsque le périphérique réseau n'est pas toujours initialisé dans le même ordre. Cependant, le nom de l'interface dépend encore de l'ordre d'initiialisation. Il y a deux manières d'assurer un accès fiable à l'interface d'une carte réseau donnée :

- /sbin/getcfg-interface ⟨*nom-de-la-configuration*⟩ retourne le nom de l'interface réseau correspondante. C'est pourquoi il est également possible d'indiquer le nom de configuration, tel que pare-feu, dhcpd, routage et diverses interfaces réseau virtuelles (tunnels), à la place du nom de l'interface (qui n'est pas persistant) dans certains fichiers de configuration, mais pas encore dans tous.
- On peut affecter un nom d'interface persistant à toute interface dont le fichier de configuration ne porte pas le nom de l'interface. Ce but est atteint par le biais de déclarations PERSISTENT_NAME=<nomp> dans un fichier de configuration d'interface (ifcfg-*). Le nom persistant ⟨*pname*⟩ ne peut en revanche pas être le même que le noyau donnerait automatiquement. Par conséquent, eth*, tr*, wlan*, qeth*, iucv*, etc. ne sont pas autorisés. Utilisez à la place net* ou des noms descriptifs tels que externe, interne ou dmz. Un nom persistant ne peut être attribué à une interface qu'immédiatement après son enregistrement, ce qui impose de recharger les pilotes des cartes réseau ou d'exécuter hwup <description-du-périphérique>). La commande rcnetwork restart ne suffit pas.

Important

Utiliser des noms d'interfaces persistants

L'utilisation des noms d'interface persistants n'a pas encore été testée dans tous les domaines. Par conséquent, iI se peut que certaines applications ne puissent pas gérer les noms d'interfaces librement choisis. Si vous êtes confronté à un problème de ce genre, veuillez nous en informer à l'aide de http://www.suse.de/feedback.

Important

ifup exige une interface existante, du fait qu'il n'initialise pas le matériel. L'initialisation du matériel est gérée par la commande hwup (exécutée par hotplug ou coldplug). Quand un périphérique est initialisé, hotplug exécute automatiquement ifup pour la nouvelle interface et cette dernière est mise en service si le mode de démarrage est onboot, hotplug ou auto et si le service network a été démarré. Auparavant, il était d'usage que la commande ifup <nom-de-l-interface> lance l'initialisation du matériel. La procédure est maintenant inversée. Un composant matériel est d'abord initialisé, puis toutes les autres actions suivent. Ainsi, il est possible de configurer un nombre variable de périphériques de manière optimale avec un ensemble de configurations existantes.

Le tableau 22.5 de la présente page résume les principaux scripts impliqués dans la configuration réseau. Dans la mesure du possible, une distinction a été faite entre interface et matériel.

TAB. 22.5: *Scripts pour la configuration manuelle du réseau*

Étape de configuration	Commande	Fonction
Matériel	hw{up,down,status}	Les scripts hw* sont appelés par le sous-système de branchement à chaud pour initialiser un périphérique, annuler son initialisation, ou demander l'état d'un périphérique. De plus amples informations sont disponibles dans man hwup.
Interface	getcfg	getcfg vous permet d'obtenir à partir du nom d'une configuration ou d'une description matérielle le nom de l'interface correspondante. De plus amples informations sont disponibles dans man getcfg.
Interface	if{up,down,status}	Les scripts if* démarrent les interfaces réseau existantes ou renvoient l'état de l'interface spécifiée. Vous trouverez plus d'informations dans la page de manuel de ifup.

Vous trouverez plus d'informations à propos des noms de périphériques persistants dans le chapitre 18 page 373 et le chapitre 19 page 383.

22.5.1 Fichiers de configuration

Cette section donne un aperçu des fichiers de configuration réseau et explique leur fonction ainsi que le format utilisé.

/etc/syconfig/hardware/hwcfg-*

Ces fichiers contiennent les configuration matérielles des cartes réseau et des autres périphériques. Ils contiennent les paramètres nécessaires, comme le module du noyau, le mode de démarrage et les associations de scripts. Pour les détails, reportez-vous à la page de manuel de `hwup`. Les configurations de `hwcfg-static-*` sont appliquées lorsque coldplug démarre, indépendamment du matériel existant.

/etc/sysconfig/network/ifcfg-*

Ces fichiers contiennent les configurations de l'interface réseau. Ils contiennent des informations telles que le mode de démarrage et l'adresse IP. Les paramètres possibles sont décrits dans la page de manuel de `ifup`. Il est également possible d'utiliser toutes les variables des fichiers `dhcp`, `wireless` et `config` dans les fichiers `ifcfg-*` si un réglage général ne doit être utilisé que pour une seule interface.

/etc/sysconfig/network/config, dhcp, wireless

Le fichier `config` contient les réglages généraux concernant le comportement de `ifup`, `ifdown` et `ifstatus`. `dhcp` contient des réglages concernant DHCP et `wireless` des réglages liés aux cartes réseau sans fil. Les variables de ces trois fichiers sont commentées et peuvent également être utilisées dans les fichiers `ifcfg-*` où elles sont prioritaires.

/etc/sysconfig/network/routes,ifroute-*

Le routage statique des paquets TCP/IP est fixé ici. Toutes les routes statiques exigées par les diverses tâches du système peuvent être indiquées dans le fichier `/etc/sysconfig/network/routes` : les routes vers un hôte, les routes vers

un hôte via une passerelle et les routes vers un réseau. Pour chaque interface nécessitant un routage individuel, définissez un fichier de configuration supplémantaire : `/etc/sysconfig/network/ifroute-*`. Remplacez `*` par le nom de l'interface. Voici à quoi ressemblent les déclarations des fichiers de configuration du routage :

```
DESTINATION
   PASSERELLE MASQUE       INTERFACE [ TYPE ] [ OPTIONS ] DESTINATION
   PASSERELLE LG_PREFIXE INTERFACE [ TYPE ] [ OPTIONS ] DESTINATION/LG_PREFIXE
   PASSERELLE -                 INTERFACE [ TYPE ] [ OPTIONS ]
```

Pour ne pas indiquer PASSERELLE, MASQUE, LG_PREFIXE ou INTERFACE, écrivez `-` à la place. Les déclarations TYPE et OPTIONS peuvent simplement être omises.

La destination de la route est dans la première colonne. Cette colonne peut contenir l'adresse IP d'un réseau, d'un hôte ou, dans le cas de serveurs de noms *accessibles*, le réseau ou le nom d'hôte pleinement qualifié.

La deuxième colonne contient la passerelle par défaut ou une passerelle par laquelle il est possible d'accéder à un hôte ou un réseau. La troisième colonne contient le masque réseau pour des réseaux ou des hôtes derrière une passerelle. Par exemple, le masque est `255.255.255.255` pour un hôte derrière une passerelle.

La dernière colonne n'est pertinente que pour les réseaux connectés à l'hôte local, comme la boucle locale, Ethernet, RNIS, PPP et le périphérique factice. Le nom du périphérique doit être saisi ici.

/etc/resolv.conf

Ce fichier indique à quel domaine l'hôte appartient (mot-clé `search`). Y figure également l'état de l'adresse du serveur de noms auquel accéder (mot-clé `nameserver`). Plusieurs noms de domaine peuvent être spécifiés. Lors de la résolution d'un nom qui n'est pas pleinement qualifié, une tentative est effectuée pour en générer un en accolant les différents éléments `search`. Utilisez plusieurs serveurs de noms en saisissant plusieurs lignes commençant chacune par `nameserver`. Faites précéder les commentaires par des caractères #. YaST enregistre le serveur de noms spécifié dans ce fichier. L'exemple 22.5 page suivante montre à quoi `/etc/resolv.conf` pourrait ressembler.

Example 22.5: `/etc/resolv.conf`

```
# Notre domaine search exemple.com
# Nous utilisons soleil (192.168.0.20) comme serveur de noms
nameserver 192.168.0.20
```

Certains services, comme `pppd` (`wvdial`), `ipppd` (`isdn`), `dhcp`(`dhcpcd` et `dhclient`), `pcmcia` et `hotplug`, modifient le fichier `/etc/resolv.conf` au moyen du script `modify_resolvconf`. Si le fichier `/etc/resolv.conf` a été temporairement modifié par ce script, il contient un commentaire prédéfini qui fournit des informations sur le service qui l'a modifié, l'endroit où le fichier d'origine a été sauvegardé et comment on peut revenir sur le mécanisme de modification automatique. Si l'on modifie plusieurs fois `/etc/resolv.conf`, le fichier imbrique les modifications successives. Vous pouvez revenir sur celles-ci proprement si cette annulation a lieu dans un ordre différent de celui dans lequel les modifications ont été introduites. Les services susceptibles d'exiger cette flexibilité comprennent `isdn`, `pcmcia` et `hotplug`.

Lorsqu'on n'a pas mis fin à un service de façon normale et propre, il est possible de restaurer le fichier original à l'aide de `modify_resolvconf`. De plus, lors de l'amorçage du système, un contrôle est effectué pour vérifier s'il ne reste pas un `resolv.conf` non nettoyé, modifié, par exemple après une panne du système, auquel cas le `resolv.conf` original (non modifié) est restauré.

YaST utilise la commande `modify_resolvconf check` pour savoir si `resolv.conf` a été modifié et avertit ensuite l'utilisateur que ses modifications seront perdues après la restauration du fichier. En dehors de cela, YaST ne compte pas sur `modify_resolvconf`, ce qui signifie que l'impact du changement de `resolv.conf` par le biais de YaST équivaut à une modification manuelle. Dans les deux cas, les changements ont un effet permanent. Les modifications demandées par les services mentionnés ne sont que temporaires.

/etc/hosts

Dans ce fichier représenté dans l'exemple 22.6 page ci-contre), les adresses IP sont affectées à des noms d'hôtes. Si aucun serveur de noms n'est mis en œuvre, il faut lister ici tous les hôtes avec lesquels une connexion IP doit être configurée. Pour chaque hôte, saisissez une ligne composée de l'adresse IP, du nom d'hôte pleinement qualifié et du nom d'hôte dans le fichier. L'adresse IP doit être placée au début de la ligne et les autres éléments séparés par des blancs et des tabulations. Les commentaires sont toujours précédés d'un caractère #.

Example 22.6: `/etc/hosts`

```
127.0.0.1 localhost
192.168.0.20 soleil.exemple.com soleil
192.168.0.1; 192.168.0.1; terre
```

/etc/networks

C'est ici que les noms de réseau sont convertis en adresses réseau. Leur format est similaire à celui du fichier `hosts`, si ce n'est que les noms de réseau précèdent les adresses. Consultez l'exemple 22.7 de la présente page).

Example 22.7: `/etc/networks`

```
loopback     127.0.0.0
localnet     192.168.0.0
```

/etc/host.conf

La résolution de noms — la traduction de noms d'hôtes et de noms de réseaux via la bibliothèque *resolver* — est contrôlée par ce fichier. On ne l'utilise que pour les programmes liés à la libc4 ou la libc5. Pour les programmes glibc actuels, reportez-vous aux réglages contenus dans le fichier `/etc/nsswitch.conf`. Un paramètre doit toujours se trouver seul dans sa propre ligne. Les commentaires sont précédés d'un caractère #. Un exemple de `/etc/host.conf` est présenté dans le tableau 22.6 de la présente page.

TAB. 22.6: *Paramètres de /etc/host.conf*

order *hosts*, *bind*	Il s'agit d'établir l'ordre de consultation des services de résolution d'un nom. Les arguments possibles sont (séparés l'un de l'autre par des espaces ou des virgules) : *hosts* : chercher dans le fichier `/etc/hosts` *bind* : accéder à un serveur de noms *nis* utiliser NIS

multi *on/off*	Détermine si un ordinateur donné peut avoir plusieurs adresses IP dans `/etc/hosts`.
nospoof *on* spoofalert *on/off*	Ces paramètres agissent sur la prévention d'*usurpation* (spoofing) du serveur de noms, mais n'ont pas d'autre impact sur la configuration réseau.
`trim nom-de-domaine`	Le nom de domaine indiqué est séparé du nom d'hôte après la résolution du nom d'hôte (si du moins le nom d'hôte comprend le nom de domaine). Cette option est utile si le fichier `/etc/hosts` ne contient que des noms provenant du domaine local, mais qui doivent quand même être être reconnus avec les noms de domaine accolés.

Example 22.8: `/etc/host.conf`

```
# Le démon named tourne
order hosts bind
# Permettre des adresses multiples
multi on
```

/etc/nsswitch.conf

La version 2.0 de la bibliothèque C de GNU a introduit le *Name Service Switch* (NSS). Reportez-vous à la page de manuel `man 5 nsswitch.conf` et au *The GNU C Library Reference Manual* pour les détails.

L'ordre des requêtes est défini dans le fichier `/etc/nsswitch.conf`. Un exemple de `nsswitch.conf` est présenté dans l'exemple 22.9 page suivante. Les commentaires sont introduits par des caractères #. Dans cet exemple, l'élément placé sous la base de données `hosts` signifie qu'une requête est envoyée à `/etc/hosts` (`files`) via DNS (reportez-vous au chapitre 24 page 463).

Example 22.9: `/etc/nsswitch.conf`

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

Les ”bases de données“ disponibles sur NSS sont répertoriées dans le tableau 22.7 de la présente page. De plus, `automount`, `bootparams`, `netmasks` et `publickey` sont attendus dans un futur proche. Les options de configuration pour les bases de données NSS sont répertoriées dans le tableau 22.8 page suivante.

TAB. 22.7: *Bases de données disponibles dans /etc/nsswitch.conf*

`aliases`	Alias de courrier utilisés par `sendmail` ; reportez-vous à la page de manuel `man 5 aliases`.
`ethers`	Adresses Ethernet.
`group`	Pour les groupes d'utilisateurs, utilisés par `getgrent`. Consultez également la page de manuel de `group`.
`hosts`	Pour les noms d'hôtes et les adresses IP, utilisés par `gethostbyname` et les fonctions similaires.
`netgroup`	Il s'agit de la liste en vigueur sur le réseau des hôtes et des utilisateurs pour le contrôle des droits d'accès ; reportez-vous à `man 5 netgroup`.

networks	Noms et adresses des réseaux utilisés par getnetent.
passwd	Mots de passe utilisateur utilisés par getpwent ; reportez-vous à la page de manuel man 5 passwd.
protocols	Protocoles réseau utilisés par getprotoent ; reportez-vous à la page de manuel man 5 protocols.
rpc	Noms et adresses d'appels de procédure distants (*Remote Procedure Call*) utilisés par getrpcbyname et d'autres fonctions similaires.
services	Services réseau utilisés par getservent.
shadow	Mots de passe *shadow* des utilisateurs utilisés par getspnam ; reportez-vous à la page de manuel man 5 shadow.

TAB. 22.8: *Possibilités de configuration des bases de données NSS*

files	accès direct à des fichiers, par exemple à /etc/aliases.
db	accès à une base de données.
nis, nisplus	NIS, reportez-vous au chapitre 25 page 485
dns	peut seulement être utilisé comme extension de hosts et networks.
compat	peut seulement être utilisé comme extension de passwd, shadow et group.

/etc/nscd.conf

Ce fichier permet de configurer nscd (name service cache daemon). Reportez-vous à `man 8 nscd` et `man 5 nscd.conf`). Par défaut, les éléments système provenant de `passwd` et `groups` sont mis en cache par nscd. C'est important pour les performances des services de répertoires comme NIS et LDAP, car sinon il faut utiliser la connexion réseau pour chaque accès aux noms ou aux groupes. `hosts` n'est normalement pas mis en cache par défaut, parce que le mécanisme contenu dans nscd pour mettre en cache les hôtes rend le système incapable de se fier aux contrôles de recherches directes ou inverses. Au lieu de demander à nscd de mettre des noms en cache, configurez un serveur de cache DNS.

Si la mise en cache de `passwd` est activée, il faut environ 15 secondes jusqu'à ce qu'un utilisateur local récemment ajouté soit reconnu. Réduisez ce temps d'attente en redémarrant nscd avec la commande `rcnscd restart`.

/etc/HOSTNAME

C'est ici que se trouve le nom d'hôte sans nom de domaine accolé. Ce fichier est lu par plusieurs scripts pendant que la machine démarre. Il ne peut contenir qu'une ligne, dans laquelle le nom d'hôte est défini.

22.5.2 Scripts de démarrage

En dehors des fichiers de configuration décrits précédemment, il y a également différents scripts qui chargent les programmes réseau pendant que la machine amorce. Ceux-ci sont démarrés dès que le système passe à un des *niveaux d'exécution multi-utilisateurs*. Certains de ces scripts sont décrits dans le tableau 22.9 de la présente page).

TAB. 22.9: *Quelques scripts de démarrage des programmes réseau*

`/etc/init.d/network`	Ce script gère la configuration des interfaces réseau. Le matériel doit déjà avoir été initialisé par `/etc/init.d/coldplug` (par le biais de `hotplug`). Si le service `network` n'a pas été démarré, aucune interface réseau n'est mise en œuvre quand elle est ajoutée au moyen de hotplug.

`/etc/init.d/xinetd`	Démarre xinetd. xinetd peut servir à mettre à disposition des services de serveur sur le système. Par exemple, il peut démarrer vsftpd chaque fois qu'une connexion FTP est initiée.
`/etc/init.d/portmap`	Démarre *portmapper*, lequel est requis pour pouvoir utiliser un serveur RPC, comme par exemple un serveur NFS.
`/etc/init.d/nfsserver`	Démarre le serveur NFS.
`/etc/init.d/sendmail`	Contrôle le processus sendmail.
`/etc/init.d/ypserv`	Démarre le serveur NIS.
`/etc/init.d/ypbind`	Démarre le client NIS.

22.6 Le démon smpppd en tant qu'assistant à la numérotation

La plupart des utilisateurs privés n'utilisent pas de connexion continue à Internet et ne composent le numéro de leur fournisseur qu'à la demande. Ce sont les applications ipppd ou pppd qui ont le contrôle sur cette connexion, selon le type de connexion (RNIS ou ADSL). Il suffit normalement de démarrer ces programmes correctement pour être en ligne.

Tant que l'utilisateur dispose d'un tarif forfaitaire qui n'entraîne aucun frais supplémentaire lors de la connexion, il suffit généralement de démarrer le démon de la manière appropriée. On souhaite cependant parfois pouvoir mieux contrôler la connexion, que ce soit à l'aide d'une applet KDE ou d'une interface à base de ligne de commande. Si la passerelle Internet n'est pas l'ordinateur de travail, il faut pouvoir gérer la connexion par l'intermédiaire d'un hôte réseau.

C'est à ce niveau qu'intervient smpppd (le méta-démon PPP de SUSE). Il met à la disposition des utilitaires une interface unique qui fonctionne dans deux directions. D'une part, il programme le démon pppd ou ipppd approprié et gère son

comportement lors de la connexion. D'autre part, il propose aux programmes utilisateur différents fournisseurs d'accès et donne des informations sur l'état actuel de la connexion. Comme le démon smpppd peut également être géré via le réseau, il est particulièrement bien approprié pour gérer la connexion à l'Internet à partir d'un poste de travail dans le sous-réseau privé.

22.6.1 Configuration du démon smpppd

YaST configure automatiquement les connexions mises à disposition par smpppd. Les programmes de connexion à proprement parler, kinternet et cinternet, sont également préconfigurés. Lorsque vous souhaitez installer des fonctionnalités supplémentaires de smpppd, comme un service distant par exemple, vous devez procéder manuellement.

Le fichier de configuration du démon smpppd se trouve dans `/etc/smpppd.conf`. Par défaut, aucun service distant n'est possible. Les options les plus intéressantes de ce fichier de configuration sont :

open-inet-socket = <yes|no> Lorsque vous souhaitez pouvoir gérer le démon smpppd via le réseau, vous devez régler cette option sur `yes`. Le port que le démon smpppd écoute alors est le port `3185`. Si ce paramètre est réglé sur `yes`, vous devez définir les paramètres `bind-address`, `host-range` et `password` en conséquence.

bind-address = <ip> Quand un ordinateur possède plusieurs adresses IP, vous pouvez décider depuis quelles adresses IP le démon smpppd accepte des connexions.

host-range = <min ip> <max ip> Vous pouvez utiliser le paramètre `host-range` pour définir un intervalle réseau. L'accès au smpppd est alors autorisé aux ordinateurs dont les adresses IP se trouvent dans cet intervalle. Tous les ordinateurs ne se trouvant pas dans cet intervalle sont rejetés.

password = <password> En donnant un mot de passe, on peut limiter les clients aux ordinateurs autorisés. Comme il s'agit d'un mot de passe en texte clair, il ne faut pas surestimer la sécurité qu'il apporte. Si aucun mot de passe n'est attribué, tous les clients sont alors autorisés à accéder au démon smpppd.

slp-register = <yes|no> Avec ce paramètre, le service du démon smpppd peut être annoncé dans le réseau via SLP.

Vous trouverez plus d'informations sur le démon smpppd dans `man 8 smpppd` et `man 5 smpppd.conf`.

22.6.2 Configuration de kinternet, cinternet et qinternet en utilisation distante

Les programmes kinternet, cinternet et qinternet peuvent être utilisés pour gérer un démon smpppd local ou distant. cinternet est en fait l'équivalent à la ligne de commandes du programme graphique kinternet. Le programme qinternet est l'équivalent de kinternet mais il n'utilise pas le bibliothèques KDE ; il peut donc être utilisé sans KDE et peut être installé séparément. Si vous souhaitez préparer ces utilitaires à utiliser un démon smpppd distant, vous devez modifier le fichier de configuration `/etc/smpppd-c.conf` manuellement ou à l'aide de kinternet. Ce fichier n'utilise que trois options :

sites = <list of sites> Ici, vous indiquez aux interfaces frontales où rechercher le démon smpppd. Les interfaces frontales essaieront les options dans l'ordre établi ici. L'option `local` renvoie à l'établissement d'une connexion au smpppd local, `gateway` à un smpppd sur la passerelle. Avec `config-file`, la connexion doit être établie comme il est spécifié dans ce fichier sous `server`. `slp` indique aux interfaces frontales de se connecter avec un smpppd trouvé via SLP.

server = <server> Vous pouvez indiquer ici l'ordinateur sur lequel smpppd est exécuté.

password = <password> Saisissez ici le mot de passe qui a aussi été choisi pour le smpppd.

Si le démon smpppd fonctionne, vous pouvez à présent essayer d'y accéder en utilisant, par exemple, la commande `cinternet --verbose --interface-list`. Si vous rencontrez encore des difficultés à ce niveau, consultez `man 5 smpppd-c.conf` et `man 8 cinternet`.

Services SLP dans le réseau

Le *Service Location Protocol* (SLP) a été développé afin de simplifier la configuration des clients reliés au réseau à l'intérieur d'un réseau local. Pour configurer un client réseau, y compris tous les services souhaités, son administrateur a traditionnellement besoin d'une connaissance détaillée des serveurs disponibles dans son réseau. Avec SLP, la disponibilité d'un type de service défini est indiquée à tous les clients du réseau local. Les applications supportant SLP peuvent utiliser les informations émises via SLP et peuvent ainsi être configurées automatiquement.

SUSE LINUX supporte l'installation de sources d'installation transmises par SLP et comporte beaucoup de services système avec support intégré pour SLP. YaST et Konqueror dispose tous les deux d'applications correspondantes pour SLP. Utilisez SLP afin de mettre à la disposition des clients connectés les fonctions centrales comme le serveur d'installation, le serveur YOU, le serveur de fichiers ou le serveur d'impression sur votre SUSE LINUX.

23.1 Enregistrement de vos propres services

Beaucoup d'applications sous SUSE LINUX disposent déjà d'un support SLP intégré par l'intermédiaire de l'utilisation de la bibliothèque `libslp`. Si vous désirez en outre rendre disponibles des services supplémentaires via SLP qui n'ont aucun support SLP intégré, plusieurs possibilités s'offrent à vous :

Enregistrement statique via `/etc/slp.reg.d`

Créez pour chaque nouveau service un fichier d'enregistrement propre. Voyez ci-dessous un exemple de ce type de fichier pour l'enregistrement d'un service scanneur :

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

La ligne la plus importante de ce fichier est ce qu'on appelle l'*URL de service*, qui commence par `service:`. Elle contient le type de service (`scanner.sane`) et l'adresse sous laquelle le service est disponible sur le serveur. ⟨*$HOSTNAME*⟩ est automatiquement remplacé par le nom d'hôte complet. Séparé par deux points, arrive ensuite le port TCP sur lequel le service concerné écoute. Indiquez maintenant, séparée de l'URL de service par des guillemets, également la langue dans laquelle le service doit être indiqué et la durée de vie de l'enregistrement en secondes. La valeur pour la durée de vie de l'enregistrement peut se situer entre `0` et `65535`. Si vous indiquez `0`, l'enregistrement ne serait pas valable, avec `65535`, il n'est pas limité.

Le fichier d'enregistrement comporte en outre les deux variables `watch-tcp-port` et `description`. La première couple l'annonce SLP du service à l'état d'activité de celui-ci (slpd contrôle l'état de ce service). La dernière variable comporte une description plus précise du service ; celle-ci est affichée dans les navigateurs appropriés.

Enregistrement statique `/etc/slp.reg`
La seule différence avec la procédure décrite plus haut est la concentration de tous les services dans un unique fichier central.

Enregistrement dynamique avec slptool
Si un enregistrement SLP doit se faire à partir des propres scripts d'un service, utilisez l'interface en lignes de commandes slptool.

23.2 Interfaces SLP dans SUSE LINUX

SUSE LINUX comporte plusieurs interfaces servant à interroger et à réutiliser les informations SLP via un réseau :

slptool slptool est un programme de lignes de commandes simple pouvant être utilisé pour transmettre des requêtes SLP sur le réseau ou également pour annoncer ses propres services. `slptool --help` énumère toutes les options et fonctions disponibles. slptool peut également être appelé à partir de scripts qui traitent les informations SLP.

Navigateur SLP YaST YaST comporte sous 'Services réseau' → 'Navigateur SLP' son propre navigateur SLP, qui liste sous forme d'arborescence graphique tous les services annoncés dans le réseau local via SLP.

Konqueror Utilisé comme nagivateur de réseau, Konqueror peut indiquer, avec l'appel `slp:/`, tous les services SLP disponibles dans le réseau local. En cliquant sur les icônes apparaissant sur la fenêtre principale, vous recevrez des informations plus précises sur le service en question.

Si vous utilisez Konqueror avec `service:/`, un clic sur l'icône correspondant dans la fenêtre du navigateur vous amène vers le service choisi.

23.3 Activer SLP

Le slpd doit fonctionner sur votre système dès que vous voulez offrir vos propres services de serveur. Pour la seule interrogation de services, un démarrage de ce

démon n'est pas nécessaire. Le démon slpd est contrôlé, comme la plupart des services système sous SUSE LINUX, via son propre script Init. Le démon est inactif par défaut. Si vous désirez l'activer pour la durée d'une session, utilisez, en tant qu'utilisateur `root`, la commande `rcslpd start` afin de le démarrer et `rcslpd stop` pour l'arrêter. Avec `restart` ou `status`, vous déclenchez un redémarrage ou une demande d'état. Si slpd doit être actif par défaut, exécutez une fois, en tant que `root`, la commande `insserv slpd`. Ainsi, slpd est automatiquement intégré dans la liste des services à démarrer lors de l'amorçage du système.

23.4 Informations supplémentaires

Pour des informations plus approfondies relatives au SLP, vous disposez des sources suivantes :

RFC 2608, 2609, 2610 RFC 2608 traite en général de la définition de SLP. RFC 2609 entre plus en détails dans la syntaxe des URL de service utilisés et RFC 2610 traite de DHCP via SLP.

http://www.openslp.com Le site du projet OpenSLP.

file:/usr/share/doc/packages/openslp/*
Vous trouverez dans ce répertoire toute la documentation disponible au sujet de SLP ainsi qu'un `README.SuSE` avec les spécification SUSE LINUX, les RFC mentionnés ci-dessus et deux documents HTML d'introduction. Les programmeurs souhaitant utiliser les fonctions SLP doivent installer le paquetage `openslp-devel` afin d'exploiter le *Guide du Programmeur* joint.

La résolution de noms

DNS (en anglais, Domain Name System) sert à résoudre les noms de domaines et de machines, c'est-à-dire à les convertir en adresses IP. De cette manière, l'adresse IP 192.168.0.1 est par exemple attribuée au nom d'hôte `terre`.Avant de configurer votre propre serveur de noms, nous vous recommandons de consulter les informations d'ordre général relatives à la résolution de noms dans la section 22.3 page 432. Les exemples de configuration suivants font référence à BIND.

24.1 Configuration avec YaST

Le module DNS de YaST sert à configurer un serveur de noms dans le réseau local. Lorsque vous démarrez le module pour la première fois, un assistant apparaît et vous demande de prendre quelques décisions fondamentales sur l'administration du serveur. Une fois la configuration initiale terminée, le serveur est sommairement configuré et prêt à l'emploi dans les grandes lignes. Le mode expert sert pour des tâches de configuration plus avancées comme les ACL, la journalisation et les clés TSIG, entre autres.

24.1.1 Configuration avec l'assistant

L'assistant se compose de trois étapes ou boîtes de dialogue. Vous pouvez entrer en mode expert à partir de chaque boîte de dialogue.

Configuration des redirecteurs Lorsque ce module démarre pour la première fois, vous voyez la boîte de dialogue montrée dans la figure 24.1 page ci-contre. Décidez-y si vous souhaitez recevoir une liste des redirecteurs lorsque vous vous connectez par ADSL ou par RNIS ('Démon PPP définit les redirecteurs'), ou les lui donner vous-même ('Spécifier les redirecteurs manuellement').

Zones DNS Les éléments de ce module sont expliqués dans l'installation en mode expert dans page 466.

Terminer avec l'assistant Dans la dernière boîte de dialogue, vous pouvez ouvrir le port DNS (port 53) dans le pare-feu activé pendant l'installation et décider si le DNS doit être démarré. Vous pouvez également accéder à la configuration en mode expert depuis cette boîte de dialogue. Reportez-vous à la figure 24.3 page 467.

24.1.2 Configuration avancée

Lorsque le module démarre pour la première fois, YaST ouvre une fenêtre offrant plusieurs possibilités de configuration. Dès que la configuration est terminée, le serveur de noms est en principe prêt à fonctionner :

Démarrage Dans la section 'Amorçage', vous pouvez définir si le serveur DNS doit être en 'Marche' ou à l''Arrêt' par défaut. Les boutons 'Démarrer le serveur DNS maintenant' et 'Arrêter le serveur DNS maintenant' permettent

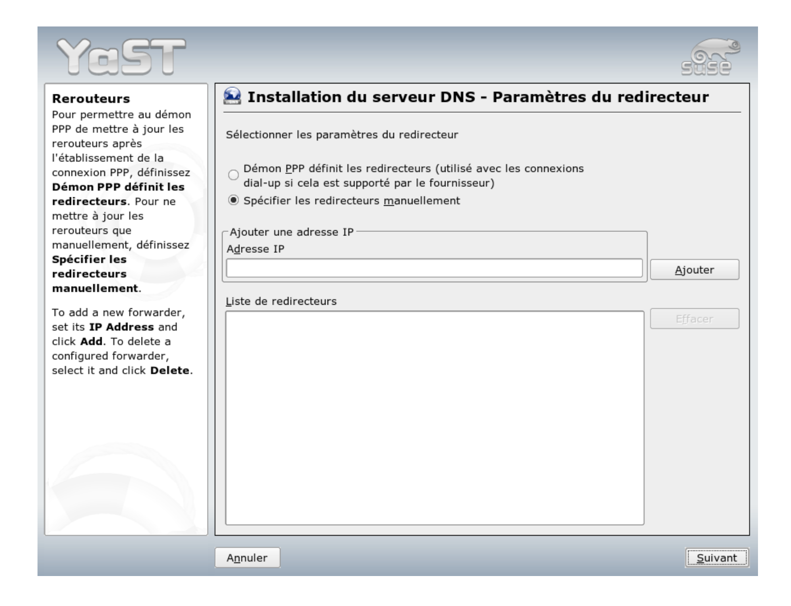


FIG. 24.1: *Installation du serveur de noms~: paramètres des redirecteurs*

respectivement de démarrer et d'arrêter le serveur de noms sur l'instant. 'Enregistrer les paramètres et redémarrer le serveur DNS maintenant' vous permet d'enregistrer la configuration actuelle. Vous pouvez ouvrir le port DNS du pare-feu ('Ouvrir port dans pare-feu') et modifier l'installation du pare-feu dans 'Paramètres du pare-feu'.

Redirecteurs Cette boîte de dialogue est identique à celle qui apparaît au démarrage de l'assistant de configuration (voir page précédente).

Journalisation Cette rubrique vous servira à paramétrer ce que le serveur de noms doit consigner dans son journal et comment. Précisez dans 'Type de journal' l'endroit où le serveur de noms doit consigner ses messages. Vous pouvez utiliser le fichier de journal global du système `/var/log/messages` en choisissant 'Journaliser dans le journal système' ou spécifier un autre fichier en choisissant 'Journaliser dans le fichier'. Dans ce cas, définissez aussi la taille maximale du fichier en méga-octets et le nombre de fichiers journaux à garder.

'Journalisations additionnelles' vous permet d'ajuster d'autres options. 'Journaliser les requêtes nommées' enregistre *chaque* requête. Le fichier journal peut donc devenir très volumineux rapidement. Vous ne devriez choisir

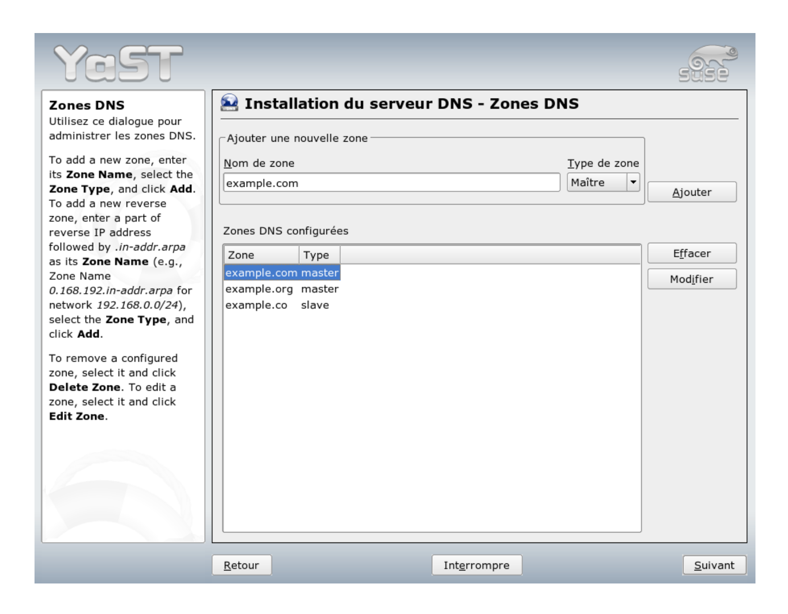


FIG. 24.2: *DNS Server Installation: DNS Zones*

cette option qu'à des fins de débogage. Pour consigner le flux de données lors des mises à jour de zones entre le serveur DHCP et le serveur DNS, choisissez l'option'Journaliser les mises à jour de zone'. Pour consigner le flux de données lors des transferts de zones du maître vers l'esclave, activez l'option 'Journaliser les transferts de zone' . Reportez-vous à la figure 24.4 page 468.

Zones DNS Cette boîte de dialogue est divisée en plusieurs parties et permet de gérer des fichiers de zones (voir la section 24.4 page 477). Dans 'Nom de zone' saisissez le nom d'une nouvelle zone. Pour créer des zones inverses, le nom de la zone doit se terminer par `.in-addr.arpa`. Choisissez le type (maître ou esclave) avec 'Type de zone' (voir la figure 24.5 page 469). Le bouton 'Modifier zone...' vous permet de modifier d'autres réglages. Lorsque vous voulez supprimer une zone, cliquez sur 'Effacer zone'.

Éditeur de zones esclaves Cette boîte de dialogue apparaît si vous avez choisi à l'étape décrite dans de la présente page 'Esclave' comme type de zone. Indiquez dans le champ 'Serveur DNS maître' le serveur maître duquel l'esclave doit obtenir ses données. Si vous souhaitez limiter l'accès au serveur, choisissez une des ACL définies au préalable dans la liste. Reportez-vous à la

FIG. 24.3: *Installation du serveur de noms~: terminer avec l'assistant*

figure 24.6 page 470.

Éditeur de zones maîtres Cette boîte de dialogue apparaît si vous avez choisi à l'étape décrite dans page précédente 'Maître' comme type de zone. Elle se subdivise en plusieurs vues : 'Basiques' (la première page ouverte), 'Enregistrements NS', 'Enregistrements MX', 'SOA' et 'Enregistrements'.

Éditeur de zones (enregistrements NS) Cette boîte de dialogue permet de définir un serveur de noms secondaire pour ces zones. Veillez à ce que le serveur de nom proprement dit soit contenu dans la liste. Pour saisir un nouvel enregistrement, indiquez dans 'Serveur de nom à ajouter' le nom correspondant et confirmez au moyen de 'Ajouter'. Reportez-vous à la figure 24.7 page 471.

Éditeur de zones (enregistrements MX) Pour ajouter un nouveau serveur de messagerie pour la zone actuelle à la liste en place, indiquez l'adresse et la valeur de priorité qui conviennent. Confirmez au moyen de 'Ajouter'. Reportez-vous à la figure 24.8 page 472).

Éditeur de zones (SOA) Cette page vous permet de créer des enregistrements SOA (*Start of Authority*). L'exemple 24.6 page 478 explique les différentes

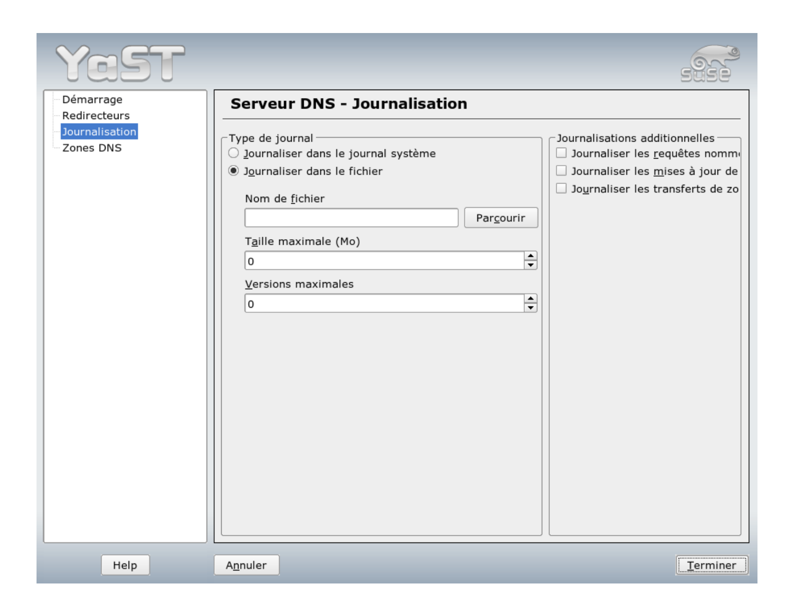


FIG. *24.4: Serveur DNS~: journalisation*

options. Il n'est pas possible de modifier les enregistrements SOA si les zones dynamiques sont gérées par LDAP.

Éditeur de zones (enregistrements) Cette boîte de dialogue vous permet de gérer une liste d'affectations de noms à des adresses IP. Indiquez dans la zone de saisie 'Nom' le nom d'hôte puis choisissez son type. 'A-Record' représente l'enregistrement principal. 'CNAME' est un alias. Dans 'MX-Relay', l'enregistrement (Nom) est remplacé par la valeur (Valeur).

24.2 Démarrer le serveur de noms BIND

Le serveur de noms BIND (*Berkeley Internet Name Domain*) est déjà configuré dans SUSE LINUX de manière à ce que vous puissiez le démarrer tout de suite après avoir effectué l'installation. Lorsque vous avez déjà une connexion Internet qui fonctionne et que vous indiquez dans le fichier `/etc/resolv.conf` le serveur de noms `127.0.0.1` pour `localhost`, vous possédez déjà, en règle générale, une résolution de noms fonctionnant parfaitement sans connaître

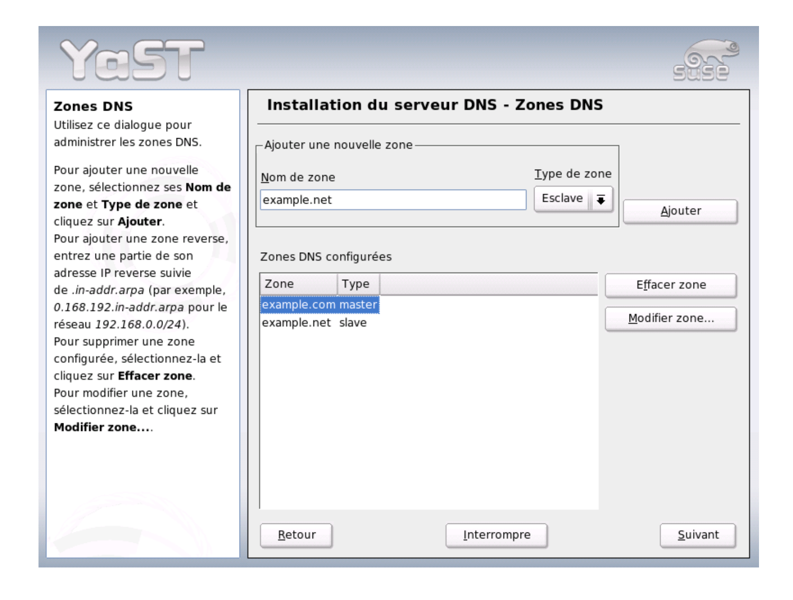


FIG. 24.5: *Serveur DNS~: zones DNS*

le DNS du fournisseur d'accès. BIND effectue alors la résolution de noms par l'intermédiaire du serveur de noms racine, ce qui est en revanche beaucoup plus lent. On devra normalement indiquer le DNS du fournisseur d'accès ainsi que son adresse IP dans le fichier de configuration `/etc/named.conf` dans la rubrique `forwarders` pour bénéficier d'une résolution de noms efficace et sûre. Tant que cela fonctionne, le serveur de noms fonctionne en tant que serveur de noms "cache seulement" (caching-only). Ce n'est que lorsque l'on mettra à sa disposition ses propres zones qu'il deviendra un véritable serveur de noms. Vous en trouverez un exemple simple dans le répertoire de documentation `/usr/share/doc/packages/bind/sample-config`.

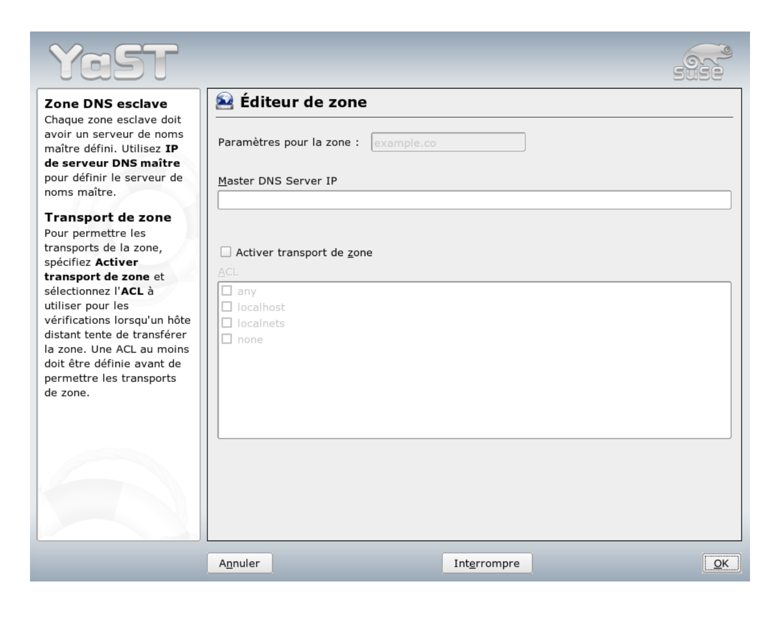


FIG. 24.6: *Serveur DNS~: éditeur de zones esclaves*

Astuce

Adaptation automatique des déclarations de serveurs de noms

Les déclarations des serveurs de noms peuvent être adaptées automatiquement à la situation, en fonction de la façon d'accéder à Internet ou de l'environnement réseau. Pour cela, positionnez la variable `MODIFY_NAMED_CONF_DYNAMICALLY` du fichier `/etc/sysconfig/network/config` à la valeur `yes`.

Astuce

Il ne faut cependant pas définir un nom de domaine officiel sans l'avoir fait au préalable approuver par l'institution compétente. Même lorsque vous disposez de votre propre domaine et qu'il est géré par votre fournisseur d'accès, nous vous recommandons de ne pas l'utiliser dans la mesure où BIND ne redirigerait plus aucune requête pour ce domaine. Le serveur web du fournisseur d'accès dédié à votre propre domaine ne pourrait par exemple plus être joint.

Pour démarrer le serveur de noms, saisissez en tant que `root` la commande `rcnamed start`. Si "done" apparaît en vert à droite, named, c'est-à-dire le

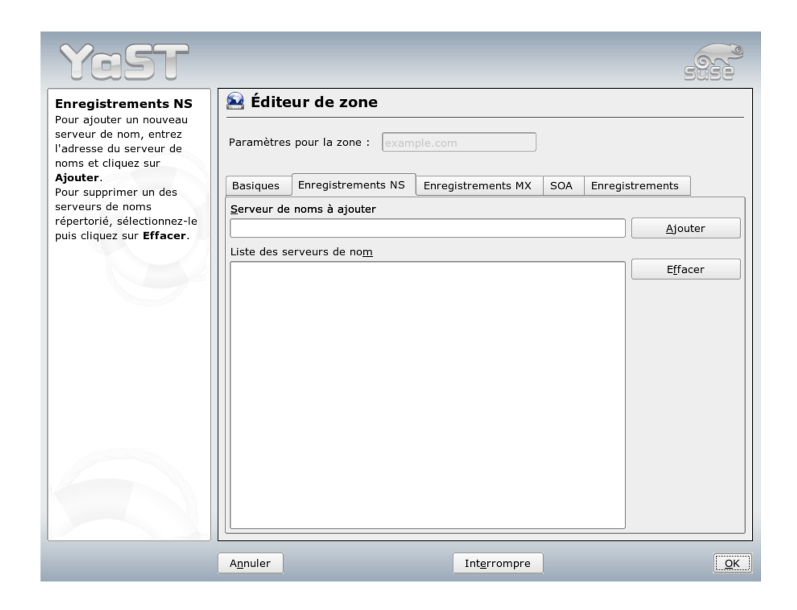


FIG. 24.7: *Serveur DNS~: éditeur de zones (enregistrements NS)*

processus du serveur de noms, est démarré avec succès. Vous pouvez tester immédiatement sur le système local le fonctionnement du serveur de noms avec les programmes `host` ou `dig` qui devraient renvoyer `localhost` comme serveur par défaut avec l'adresse `127.0.0.1`. Si tel n'était pas le cas, cela signifierait qu'un mauvais nom de serveur figure probablement dans le fichier `/etc/resolv.conf` ou que ce fichier n'existe tout simplement pas. Testez pour commencer `host 127.0.0.1`, qui devrait normalement toujours fonctionner. Si vous obtenez un message d'erreur, utilisez la commande `rcnamed status` pour vérifier que le processus `named` a bien été lancé. Si le serveur de noms ne démarre pas ou se comporte de manière inattendue, vous en trouverez normalement la cause dans le fichier `/var/log/messages`.

Pour utiliser en tant que redirecteur (forwarder) le serveur de noms du fournisseur d'accès ou un de vos propres serveurs de noms déjà en service sur votre réseau local, il faut indiquer la ou les adresses IP correspondantes dans la section `options` avec le mot-clé `forwarders`. Les adresses IP utilisées dans l'exemple 24.1 page suivante sont choisies de manière arbitraire et doivent être adaptées à vos propres besoins.

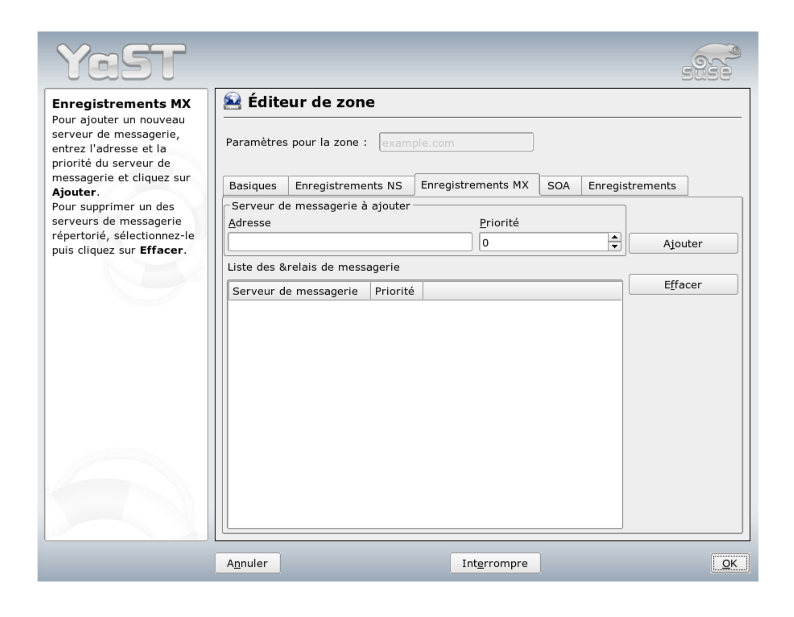


FIG. 24.8: *Serveur DNS~: éditeur de zones (enregistrements MX)*

Example 24.1: *Options de redirection (forwarding) dans named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.11.12.13; 10.11.12.14; };
        listen-on { 127.0.0.1; 192.168.0.99; };
        allow-query { 127/8; 192.168.0/24; };
        notify no;
        };
```

Après les `options` viennent les déclarations de zones, `localhost` et`0.0.127.in-addr.arpa`. L'enregistrement `type hint` situé sous ".“ doit toujours être présent. Les fichiers correspondants ne doivent pas être modifiés et ils devraient fonctionner en l'état. Vous devez veiller également à ce que chaque ligne soit suivie d'un `;` et que les accolades soient placées correctement. Si vous avez entrepris des modifications dans le fichier de configuration `/etc/named.conf` ou dans les fichiers des zones, vous devez ordonner à BIND

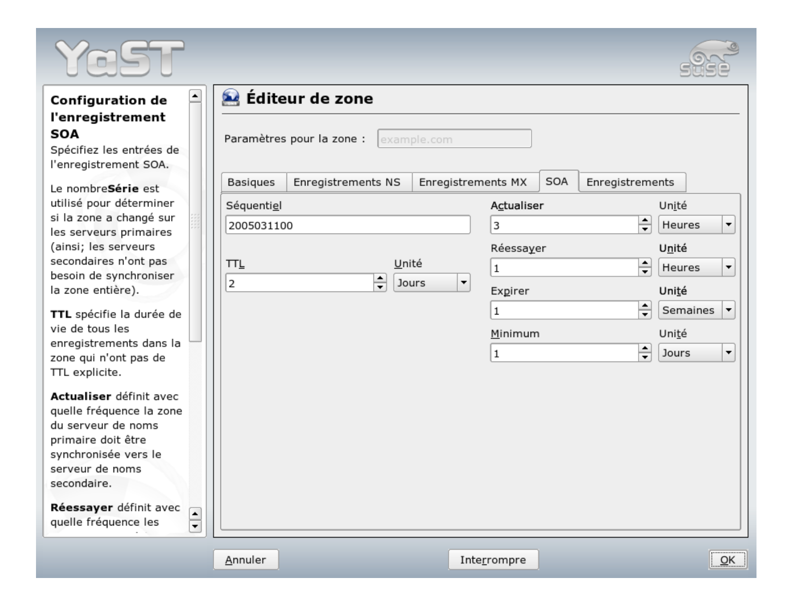


FIG. 24.9: *Serveur DNS~: éditeur de zones (SOA)*

de les lire à nouveau à l'aide de la commande `rcnamed reload`. Vous pouvez arriver au même résultat en redémarrant complètement le serveur de noms avec la commande `rcnamed restart`. Vous pouvez arrêter à tout moment le serveur de noms avec la commande `rcnamed stop`.

24.3 Le fichier de configuration /etc/named.conf

Tous les paramétrages du serveur de noms BIND sont enregistrés dans le fichier `/etc/named.conf`. Les données de zone, les noms des machines, les adresses IP, etc. des domaines à gérer sontenregistrées dans des fichiers séparés du répertoire `/var/lib/named`. Vous trouverez davantage d'informations à ce sujet plus loin.

Le fichier `/etc/named.conf` se divise principalement en deux parties : d'une part, la section `options` pour les paramètres d'ordre général et, d'autre part, les

déclarations de zone des différents domaines. La section logging (journalisation) et les déclarations d'acl (contrôle d'accès) sont optionnelles. Les lignes de commentaires commencent par le signe dièse # ou par une barre de division //. L'exemple 24.2 de la présente page présente un fichier /etc/named.conf minimaliste.

Example 24.2: *Fichier /etc/named.conf minimaliste*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

24.3.1 Les options de configuration importantes

directory "⟨*nom*⟩" indique le répertoire dans lequel BIND trouve les fichiers contenant les données de zones. Il s'agit en général de /var/lib/named.

forwarders { ⟨*adresse-ip*⟩; }; indique les serveurs de noms (la plupart du temps ceux du fournisseur d'accès) vers lesquels on redirige les requêtes DNS auxquelles il n'est pas possible de répondre directement. À la place d'⟨*adresse-ip*⟩ vous devez mettre une adresse IP comme 10.0.0.1.

forward first; a pour effet que les requêtes DNS sont redirigées avant même que le serveur de noms racine n'essaie de les résoudre. Vous pouvez utiliser forward only à la place de forward first pour que toutes les

requêtes soient redirigées et que le serveur de noms racine ne soit plus du tout consulté. Cela peut se révéler utile pour la configuration des pare-feu.

listen-on port 53 { 127.0.0.1; ⟨*adresse-ip*⟩; };
indique à BIND sur quelles interfaces réseau et sur quel port il doit écouter les requêtes des clients. Vous n'êtes pas obligé de saisir `53` dans la mesure où 53 est de toute façon le port par défaut. `127.0.0.1` permet d'accepter les requêtes de la machine locale. Si vous omettez complètement cette ligne, par défaut toutes les interfaces sont utilisées.

listen-on-v6 port 53 { any; }; indique à BIND sur quel port il doit écouter les requêtes des clients qui utilisent IPv6. Outre `any`, seul `none` est également autorisé car le serveur écoute toujours l'adresse joker IPv6.

query-source address * port 53; Cette directive peut être utile lorsqu'un pare-feu bloque les requêtes DNS externes. Cela oblige BIND à effectuer ses requêtes vers l'extérieur à partir du port 53 et pas des ports supérieurs à 1024.

query-source-v6 address * port 53; Cette directive doit être utilisée pour les requêtes basées sur IPv6.

allow-query { 127.0.0.1; ⟨*réseau*⟩; }; précise les réseaux à partir desquels les clients ont le droit d'envoyer des requêtes DNS. Il faut mettre à la place de ⟨*réseau*⟩ une adresse de la forme `192.168.1/24` où `/24` est un raccourci pour le nombre de bits dans le masque réseau, soit dans ce cas `255.255.255.0`.

allow-transfer { ! *; }; détermine quels ordinateurs sont autorisés à effectuer des transferts de zone. Cet exemple les interdit complètement du fait de la présence de `! *`. Sans cette directive, il est possible de réaliser des transferts de zone sans aucune limitation et depuis n'importe où.

statistics-interval 0; Sans cette directive, BIND produit toutes les heures plusieurs lignes de messages de statistiques dans `/var/log/messages`. Paramétrez-la à `0` pour les supprimer complètement ou spécifiez un intervalle en minutes.

cleaning-interval 720; Cette option définit au bout de quel intervalle BIND vide son cache. Cette action est à chaque fois consignée dans un enregistrement du fichier `/var/log/messages`. Le temps est indiqué ici en minutes. La valeur par défaut est de 60 minutes.

interface-interval 0; BIND parcourt régulièrement les interfaces réseau pour détecter de nouvelles interfaces ou celles qui ne sont plus disponibles. Réglez cette valeur à `0` pour l'en empêcher et pour que BIND n'écoute que les interfaces trouvées au démarrage. Vous pouvez aussi préciser l'intervalle en minutes. La valeur par défaut est de 60 minutes.

notify no; Le `no` signifie qu'aucun autre serveur de noms n'est averti en cas de modifications apportées aux données de zone ou lors du redémarrage du serveur de noms.

24.3.2 journalisation

BIND vous permet de configurer complètement ce qui est consigné dans un journal, comment et à quel endroit. Les paramétrages par défaut sont normalement suffisants. L'exemple 24.3 de la présente page montre la forme la plus simple d'une telle directive et permet d'empêcher complètement la journalisation.

Example 24.3: *La journalisation est désactivée*

```
logging {
        category default { null; };
};
```

24.3.3 Déclarations de zones

Example 24.4: *Déclaration de zone pour mon-domaine.fr*

```
zone "mon-domaine.fr" in {
       type master;
       file "mon-domaine.zone";
       notify no;
};
```

Après le mot-clé `zone`, on indique le nom du domaine géré (`mon-domaine.fr`), suivi de `in` puis, entre accolades, d'un bloc d'options qui s'appliquent à ce domaine comme le montre l'exemple 24.4 de la présente page. Si vous souhaitez définir une *zone esclave* (slave), changez la valeur du `type` en `slave` et indiquez un serveur de noms qui gère cette zone en tant que `maître` (master) (qui peut à son tour être l'esclave d'un autre maître) comme le montre l'exemple 24.5 page suivante.

Example 24.5: *Déclaration de zone pour autre-domaine.fr*

```
zone "autre-domaine.fr" in {
        type slave;
        file "slave/autre-domaine.zone";
        masters { 10.0.0.1; };
};
```

Les options de zones :

type master; Le mot-clé `master` indique que cette zone est gérée par ce serveur de noms. Cela suppose que l'on dispose d'un fichier de zone correct.

type slave; Cette zone est transférée depuis un autre serveur de noms. Elle doit être utilisée en conjonction avec des serveurs maîtres.

type hint; La zone `.` de type `hint` est utilisée pour indiquer le serveur de noms racine. Vous pouvez laisser cette définition de zone telle quelle.

file "mon-domaine.zone" ou file "slave/autre-domaine.zone"; Cette déclaration indique le fichier dans lequel figurent les données de zone du domaine. Dans le cas d'un esclave, ce fichier n'est pas nécessaire car son contenu est récupéré sur un autre serveur de noms. Pour bien distinguer les fichiers maîtres des fichiers esclaves, on place les fichiers esclaves dans le répertoire `slave`.

masters { ⟨*adresse-ip-du-serveur*⟩; }; Cette directive n'est utile que pour les zones esclaves et elle indique depuis quel serveur de noms le fichier de zones doit être transféré.

allow-update { ! *; }; Cette option régit l'accès en écriture depuis l'extérieur, ce qui permettrait à des clients de s'inscrire eux-mêmes dans le DNS — ce qui, pour des raisons de sécurité, n'est normalement pas souhaitable. Lorsque cette directive n'est pas présente, les mises à jour des zones ne sont pas autorisées du tout. Dans cet exemple, cela ne changerait rien non plus dans la mesure où `! *` interdit également toute action de ce type.

24.4 Fichiers de zone

Deux types de fichiers de zones sont nécessaires. Le premier sert à associer l'adresse IP au nom de l'ordinateur. L'autrefonctionne en sens inverse et fournit, pour une adresse IP donnée, le nom de l'ordinateur.

Astuce

Point (.) dans les fichiers de zones

Le `.` a une signification importante dans le fichier de zones. Si vous indiquez les noms des ordinateurs sans `.` final, la zone ajoutée à la fin. Il est donc important de terminer les noms d'ordinateurs complets par un `.` final, pour que le domaine n'y soit pas encore ajouté. Un point oublié ou mal placé est probablement la cause la plus fréquente d'erreur dans la configuration des serveurs de noms.

Astuce

Considérons, tout d'abord, le fichier de zone `monde.zone`, responsable du domaine `monde.entier`, montré dans l'exemple 24.6 de la présente page.

Example 24.6: *Fichier /var/lib/named/monde.zone*

```
1  $TTL 2D
2  monde.entier.   IN SOA      gateway  root.monde.entier. (
3              2003072441  ; serial
4              1D          ; refresh
5              2H          ; retry
6              1W          ; expiry
7              2D )        ; minimum
8
9              IN NS       gateway
10             IN MX       10 soleil
11
12 gateway     IN A        192.168.0.1
13             IN A        192.168.1.1
14 soleil       IN A        192.168.0.2
15 lune        IN A        192.168.0.3
16 terre        IN A        192.168.1.2
17 mars        IN A        192.168.1.3
18 www         IN CNAME    lune
```

Ligne 1 : `$TTL` définit la durée de vie par défaut (en anglais, Time To Live), c'est-à-dire la durée de vie valable de toutes les directives de ce fichier : 2 jours (2D = 2 days).

Ligne 2 : C'est ici que commence l'`enregistrement de contrôle SOA` (SOA = Start of Authority) :

- En première position, on trouve le nom du domaine à gérer `monde.entier`, ce dernier se terminant par un `.` car sinon la zone serait à nouveau ajoutée. Sinon, on peut aussi écrire ici un `@` pour que la zone de la directive correspondante soit extraite du fichier `/etc/named.conf`.
- Après `IN SOA`, on trouve le nom du serveur de noms qui sert de maître pour cette zone. Dans ce cas, le nom `gateway` est complété pour devenir `gateway.monde.entier` car il ne se termine pas par un `.`.
- Vient ensuite l'adresse électronique de la personne responsable du serveur de noms. Comme le signe `@` a déjà une signification particulière, il faut simplement écrire un `.` à la place. Ainsi, pour `root@monde.entier`, on écrit `root.monde.entier.`. N'oubliez pas le `.` à la fin, sans quoi la zone serait à nouveau ajoutée.
- Vient enfin une parenthèse `(` qui permet d'englober les lignes qui suivent jusqu'à la parenthèse `)` dans l'enregistrement SOA.

Ligne 3 : Le `numéro de série` est un nombre arbitraire qui doit être incrémenté à chaque modification de ce fichier. Il sert à informer les serveurs de noms secondaires (serveurs esclaves) des modifications entreprises. On a donc introduit pour ce faire un nombre à dix chiffres composé de la date et d'un numéro d'ordre de la forme `AAAAMMJJNN`.

Ligne 4 : La `fréquence d'actualisation` indique à quels intervalles le serveur de noms secondaire vérifie le `numéro de série` de la zone. Dans cet exemple, on a pris 1 jour (1D = 1 day).

Ligne 5 : La `fréquence des tentatives` indique l'écart de temps qui s'écoule avant qu'un serveur de noms secondaire, en cas d'erreur, n'essaie de contacter à nouveau le serveur principal. Dans le cas présent, on a 2 heures (2H = 2 hours).

Ligne 6 : La `durée d'expiration` indique la durée au bout de laquelle un serveur de noms secondaire jette les données mises en cache s'il n'a plus réussi à contacter le serveur principal. Dans le cas présent, il s'agit d'une semaine (1W = 1 week).

Ligne 7 : La dernière ligne du SOA est la `durée de vie de mise en cache des échecs`. Elle indique combien de temps les résultats des requêtes DNS des autres serveurs qui n'ont pu être résolues peuvent être conservées en mémoire cache.

Ligne 9 : `IN NS` indique le serveur de noms responsable de ce domaine. Ici aussi, le nom `gateway` est complété pour devenir `gateway.monde.entier` car il ne se termine pas par un `.`. On peut utiliser plusieurs lignes de ce type, une pour le serveur principal et une pour

chaque serveur de noms secondaire. Si `notify` dans le fichier `/etc/named.conf` ne vaut pas `no`, tous les serveurs de noms indiqués ici sont informés des modifications des données de la zone.

Ligne :10 : L'enregistrement MX indique le serveur de messagerie qui prend en charge, modifie et redirige les messages pour le domaine `monde.entier`. Dans cet exemple, il s'agit de l'ordinateur `soleil.monde.entier`. Le chiffre qui précède le nom de l'ordinateur est la valeur de préférence. Ainsi, s'il existe plusieurs déclarations MX, c'est le serveur de messagerie dont la valeur de préférence est la plus petite qui est pris, et si la remise de courrier à ce serveur échoue, on essaie celui ayant la valeur plus élevée suivante.

Lignes 12 à 17 : Il s'agit là des véritables enregistrements d'adresses (en anglais, address records), dans lesquels on attribue une ou plusieurs adresses IP à un nom d'ordinateur. Les noms figurent ici sans `.` final, car ils sont indiqués sans domaine à leur suite et sont donc tous complétés par `monde.entier`. Deux adresses IP sont attribuées à l'ordinateur `gateway` car il est équipé de deux cartes réseau. Le `A` indique une adresse de machine traditionnelle ; on utilise `A6` pour les adresses IPv6 (`AAAA` est un format dépassé pour les adresses IPv6).

Ligne 18 : On peut utiliser l'alias `www` pour désigner `lune` (`CNAME` = `canonical name`, nom canonique).

Pour la résolution inverse (en anglais, reverse lookup) des adresses IP en noms de machines, on utilise le pseudo-domaine `in-addr.arpa`. Ce dernier est ajouté à l'adresse réseau écrite dans l'ordre inverse. `192.168.1` devient donc `1.168.192.in-addr.arpa`. Reportez-vous à l'exemple 24.7 de la présente page.

Example 24.7: *Résolution inverse*

```
1  $TTL 2D 1.168.192.in-addr.arpa. IN SOA gateway.monde.entier.
2  root.monde.entier. ( 2003072441      ; serial 1D              ; refresh 2H
3  ; retry 1W              ; expiry 2D )            ; minimum IN NS
4  gateway.monde.entier. 1                      IN PTR
5  gateway.monde.entier. 2                      IN PTR
6  terre.monde.entier. 3                      IN PTR
7  mars.monde.entier.
```

Ligne 1 : $TTL définit la durée de vie par défaut valable ici pour toutes les directives.

Ligne 2 : Ce fichier permet en principe la résolution inverse pour le réseau `192.168.1.0`. Comme la zone s'appelle ici `1.168.192.in-addr.arpa`, on ne souhaite bien entendu pas l'ajouter au nom d'hôte. C'est pourquoi on saisit ce dernier en entier—avec le domaine et le `.` final. Le reste correspond à ce qui a déjà été décrit dans l'exemple précédent pour la zone `monde.entier`.

Lignes 3 à 7 : Voir l'exemple précédent pour `monde.entier`.

Ligne 9 : Cette ligne indique ici aussi à nouveau le serveur de noms responsable de cette zone, mais cette fois-ci, le nom est indiqué en entier, avec le domaine et le `.` final.

Lignes 11 à 13 : Il s'agit d'enregistrements pointeurs (pointer records) qui, pour une adresse IP pointent vers le nom d'ordinateur correspondant. On trouve au début de cette ligne uniquement le dernier chiffre de l'adresse IP, sans `.` final. Si l'on y ajoute la zone et que l'on fait abstraction de `.in-addr.arpa`, on obtient bien l'adresse IP complète en ordre inversé.

Les transferts de zones entre différentes versions de BIND ne doivent, normalement, pas poser de problème.

24.5 Actualisation dynamique des données de zones

La mise à jour dynamique (en anglais, dynamic update) est le terme technique qui décrit l'ajout, la modification et la suppression de directives dans les fichiers de zones d'un serveur maître. Ce mécanisme est décrit dans le document RFC 2136. Les mises à jour dynamiques se configurent, par zone, à l'aide des options `allow-update` ou `update-policy` au niveau des déclarations des zones. Vous ne devez pas modifier manuellement les zones mises à jour de manière dynamique.

La commande `nsupdate` sert à transmettre au serveur les enregistrements à mettre à jour. Pour connaître sa syntaxe exacte, reportez-vous à la page de manuel de `nsupdate` (`man 8 nsupdate`). Pour des raisons de sécurité, la mise à jour doit impérativement s'effectuer au moyen de transactions sécurisées (TSIG) comme décrit dans la section 24.6 page suivante.

24.6 Transactions sécurisées

On peut effectuer des transactions sécurisées avec les ”signatures de transactions“ (TSIG, transaction SIGnatures). On utilise, pour ce faire, des clés de transaction (en anglais, transaction keys) et des signatures de transaction (en anglais, transaction signatures). La section suivante explique comment les générer et les utiliser.

Les transactions sécurisées sont nécessaires dans le cadre de la communication d'un serveur à un autre et pour l'actualisation dynamique des données de zones. Un contrôle d'accès fondé sur des clés permet d'obtenir un niveau de sécurité bien plus élevé qu'un contrôle fondé sur les adresses IP.

Vous pouvez générer une clé de transaction avec la commande suivante (pour plus d'informations, cf. la page de manuel relative à la commande `dnssec-keygen`) :

dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2

Cette commande génère deux fichiers portant, par exemple, les noms suivants :

```
Khost1-host2.+157+34265.private
Khost1-host2.+157+34265.key
```

La clé (par exemple `ejIkuCyyGJwwuN3xAteKgg==`) est contenue dans les deux fichiers. Pour une utilisation ultérieure, `Khost1-host2.+157+34265.key` doit être transmis, de préférence par un chemin sécurisé à l'ordinateur distant (par exemple avec `scp`). La clé doit être ajoutée dans le fichier `/etc/named.conf` de l'hôte distant pour établir une communication sécurisée entre `host1` et `host2` :

```
key host1-host2. {
  algorithm hmac-md5;
  secret "ejIkuCyyGJwwuN3xAteKgg==";
};
```

Avertissement

Droits d'accès de `/etc/named.conf`

Veillez à ce que les droits d'accès au fichier `/etc/named.conf` restent restreints. La valeur par défaut est `0640` pour `root` et le groupe `named`. Vous pouvez aussi stocker la clé dans un fichier protégé indépendant pour l'inclure ensuite dans le fichier `/etc/named.conf`.

Avertissement

Pour que la clé pour `host2` soit utilisée sur le serveur `host1` avec, par exemple, l'adresse `192.168.2.3`, il faut saisir, sur le serveur, dans le fichier `/etc/named.conf`, les informations suivantes :

```
server 192.168.2.3 {
  keys { host1-host2. ;};
};
```

Il faut aussi saisir des directives similaires dans les fichiers de configuration de `host2`.

Pour effectuer des transactions sécurisées, il faut, en plus des ACL (listes de contrôle d'accès, à ne pas confondre avec les ACL du système de fichiers) basées sur les adresses et les intervalles d'adresses IP, ajouter des clés TSIG. L'enregistrement correspondant peut se présenter ainsi :

```
allow-update { key host1-host2. ;};
```

Pour en savoir plus, consultez le *Manuel de référence de l'administrateur BIND* sous `update-policy`.

24.7 Sécurité de DNS

DNSSEC (en anglais, DNS Security, sécurité de DNS) est décrite dans le document RFC 2535 . Le manuel de BIND décrit les outils disponibles permettant d'utiliser DNSSEC.

Une zone sûre doit posséder une ou plusieurs clés de zones. Utilisez la commande `dnssec-keygen` pour les générer, à l'instar des clés d'hôte. On utilise actuellement DSA pour générer les clés. Les clés publiques doivent être intégrées dans le fichier de zone correspondant avec une directive `$INCLUDE`.

Toutes les clés sont regroupées en un ensemble à l'aide de la commande `dnssec-makekeyset`, lequel doit être acheminé jusqu'à la zone parent (parent zone) par un chemin sûr pour y être signé à l'aide de la commande `dnssec-signkey`. Les fichiers générés lors de cette signature doivent être utilisés pour signer les zones avec la commande `dnssec-signzone` et les fichiers en résultant doivent finalement être intégrés au fichier `/etc/named.conf` pour chaque zone.

24.8 Informations supplémentaires

Nous vous recommandons notamment de consulter le *Manuel de référence de l'administrateur BIND* que vous trouverez en ligne dans `/usr/share/doc/packages/bind/`, ainsi que les RFC mentionnés dans ce dernier et les pages de manuel fournies avec BIND. Vous trouverez des informations à jour concernant la configuration de BIND sous SUSE LINUX dans `/usr/share/doc/packages/bind/README.SuSE`.

Utiliser NIS

Lorsque plusieurs systèmes UNIX d'un réseau donné veulent accéder à des ressources communes, il est nécessaire de s'assurer que les numéros des utilisateurs et des groupes sont cohérents sur toutes les machines. Le réseau doit être transparent pour l'utilisateur : quelle que soit la machine sur laquelle l'utilisateur se trouve, ce dernier doit toujours retrouver le même environnement. Ceci est rendu possible par les services NIS et NFS. Le service NFS est chargé du partage des systèmes de fichiers en réseau. Il est présenté dans chapitre 26 page 491.

NIS (en anglais Network Information Service, service d'informations réseau) peut être envisagé comme un service de base de données qui permet d'accéder aux informations contenues dans les fichiers `/etc/passwd`, `/etc/shadow` et `/etc/group` en réseau. NIS peut aussi être utilisé pour d'autres tâches (par exemple pour partager le contenu de fichiers comme `/etc/hosts` ou `/etc/services`), que nous ne détaillerons cependant pas dans cet ouvrage. On utilise souvent *YP* comme synonyme de NIS, car il joue le rôle des ”pages jaunes“ (yellow pages) du réseau.

25.1 Configurer des serveurs NIS

Pour configurer NIS, choisissez 'NIS Server' dans le module de YaST 'Services réseau'. Si votre réseau ne comporte pas encore de serveur NIS, vous devez activer l'option 'Installer et configurer un serveur NIS maître' dans le formulaire de saisie qui s'ouvre alors. Si vous avez déjà un serveur NIS (c'est-à-dire un serveur *maître*), vous pouvez ajouter un serveur NIS esclave (par exemple si vous créez un nouveau sous-réseau). Examinons tout d'abord la configuration du serveur maître.

S'il manque des paquetages, YaST vous demandera d'insérer le CD ou le DVD correspondant afin d'installer automatiquement les paquetages. Saisissez le nom de domaine en haut formulaire de saisie, illustré dans figure 25.1 de la présente page. Cochez les cases situées en dessous pour indiquer si le serveur NIS doit être aussi un client NIS pour permettre aux utilisateurs de se connecter et d'accéder à leurs données sur cette machine.

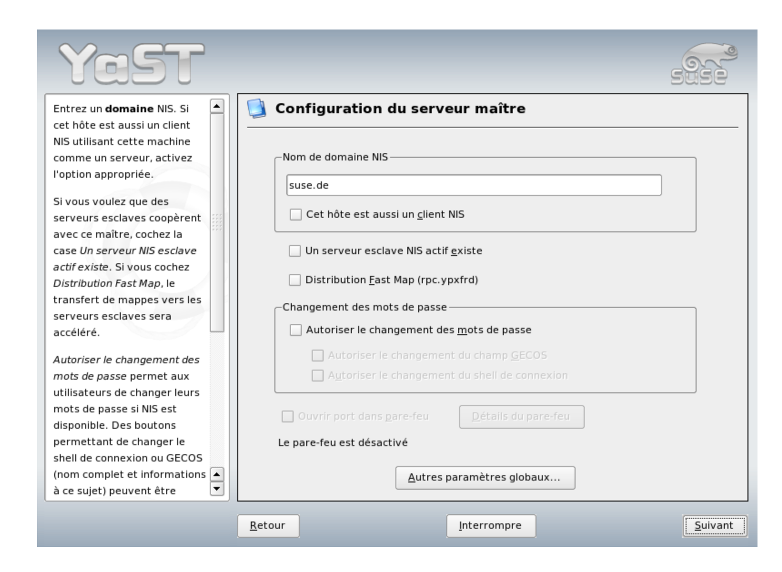


FIG. 25.1: *Utilitaire de configuration du serveur NIS*

Si vous souhaitez configurer des serveurs NIS supplémentaires ("serveurs esclaves") dans votre réseau, vous devez cocher la case 'Un serveur NIS esclave

actif existe'. Vous devez aussi cocher la case 'Distribution Fast Map' qui a pour effet de transmettre rapidement les éléments de base de données du maître aux serveurs esclave.

Si vous souhaitez autoriser les utilisateurs de votre réseau (les utilisateurs locaux et ceux qui sont gérés par le serveur NIS) à pouvoir modifier leurs mots de passe (avec la commande `yppasswd`), activez l'option correspondante. Les cases à cocher 'Autoriser le changement du champ GECOS' et 'Autoriser le changement du shell de connexion' sont alors aussi activées. "GECOS" signifie que l'utilisateur peut également modifier son nom et ses coordonnées avec la commande `ypchfn`. "SHELL" signifie qu'il peut aussi modifier son interpréteur de commandes par défaut avec la commande `ypchsh`, pour passer par exemple de bash à sh.

Lorsque vous cliquez sur 'Autres paramètres globaux...', vous arrivez dans une boîte de dialogue, illustrée dans figure 25.2 page suivante dans laquelle vous pouvez modifier le répertoire source du serveur NIS (par défaut `/etc`). Vous pouvez aussi y rassembler des mots de passe et des groupes. Laissez le réglage sur 'Oui' pour synchroniser les différents fichiers (`/etc/passwd` et `/etc/shadow` ou `/etc/group`). Vous pouvez aussi définir les plus petits numéros d'utilisateurs et de groupes pouvant être utilisés. Cliquez sur 'OK' pour confirmer les informations que vous avez saisies et pour revenir au formulaire précédent. Cliquez alors sur 'Suivant'.

Dans le cas où vous avez précédemment coché la case 'Un serveur esclave NIS actif existe', vous devez à présent indiquer le nom des machines devant faire fonction d'esclave. Cliquez ensuite sur 'Suivant'. Si vous n'utilisez pas de serveur esclave, la configuration pour le serveur est sautée et vous arrivez directement à la boîte de dialogue pour la configuration de la base de données. Indiquez-y les "tables de correspondance" (en anglais maps), autrement dit les parties de base de données qui doivent être transférées du serveur NIS au client correspondant. Les paramètres par défaut sont généralement les bons.

Après avoir cliqué sur 'Suivant', vous arrivez à la dernière boîte de dialogue, illustrée dans figure 25.3 page 489. Indiquez à partir de quels réseaux les requêtes adressées au serveur NIS seront émises. Il s'agit normalement de votre réseau d'entreprise. Vous devriez alors avoir les deux lignes suivantes :

```
255.0.0.0 127.0.0.0
0.0.0.0   0.0.0.0
```

La première ligne autorise les connexion depuis votre propre machine, qui est le serveur NIS. La seconde permet à toutes les machines ayant accès au réseau d'envoyer des requêtes au serveur.

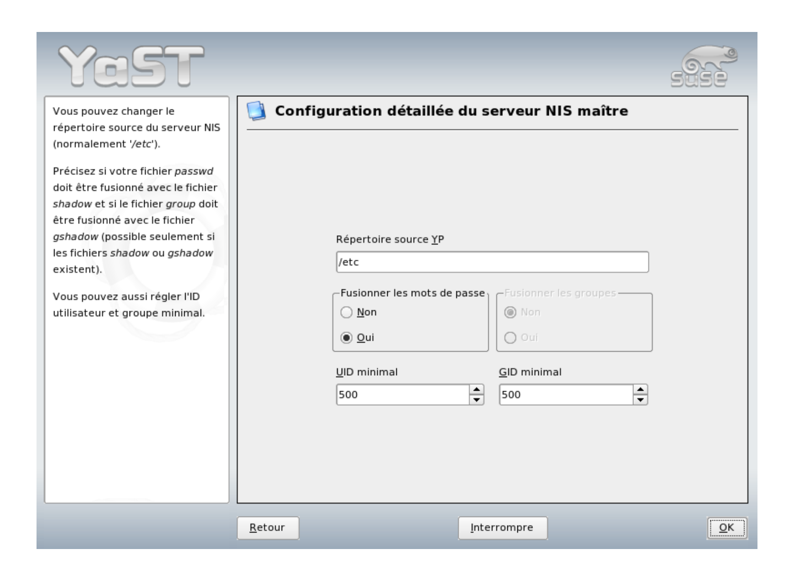


FIG. 25.2: *Serveur NIS~: changer de répertoire et synchroniser les fichiers*

Important

Configuration automatique du pare-feu

Si un pare-feu (SuSEfirewall2) fonctionne sur votre système, YaS-Tadapte sa configuration pour le serveur NIS en activant le service `portmap` dès que vous sélectionnez 'Ouvrir ports dans le pare-feu'.

Important

25.2 Configurer des clients NIS

Ce module vous permet de configurer le client NIS. Après avoir choisi d'utiliser le serveur NIS et, selon les circonstances, automounter, cette boîte de dialogue s'ouvre. Indiquez-y si le client NIS possède une adresse IP statique ou s'il doit la recevoir par DHCP. DHCP fournit également le domaine NIS et le serveur NIS. Pour plus d'informations sur le DHCP, reportez-vous à chapitre 27 page 499. Si vous utilisez une adresse IP statique, vous devez spécifier le domaine NIS et le

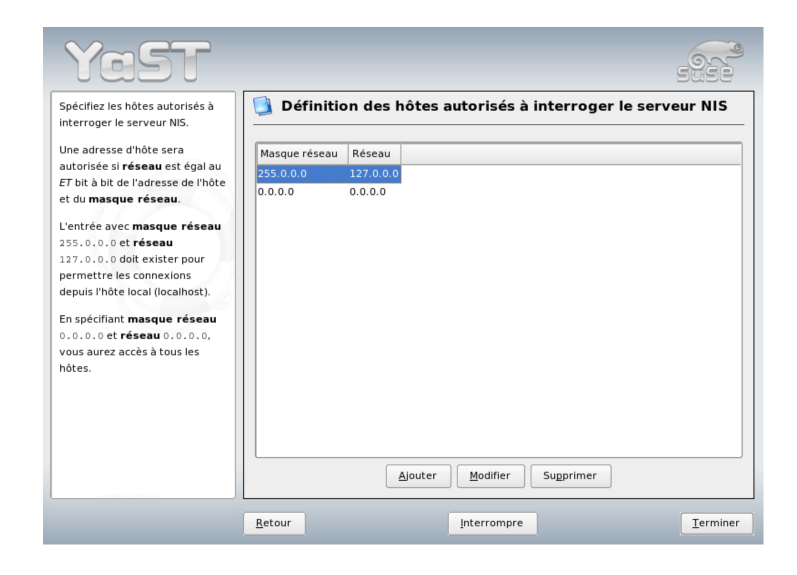


FIG. 25.3: *Serveur NIS~: définition d'une autorisation de requête*

serveur NIS manuellement. Reportez-vous à figure 25.4 page suivante. 'Chercher' demande à YaST de chercher un serveur NIS actif dans votre serveur.

Vous avez également la possibilité de spécifier des domaines multiples ainsi qu'un domaine par défaut. Pour les différents domaines, vous pouvez utiliser le bouton 'Ajouter' pour déclarer plusieurs serveurs ainsi que la fonction de diffusion (broadcast).

Vous pouvez éviter, dans la configuration experte, qu'une autre machine du réseau puisse demander quel serveur votre client utilise en cochant la case 'Répondre seulement à l'hôte local'. Si vous activez 'Serveur défectueux', les réponses provenant d'un serveur sur un port non privilégié sont acceptées. Vous pourrez consulter les détails à ce sujet dans la page de manuel de `ypbind`.

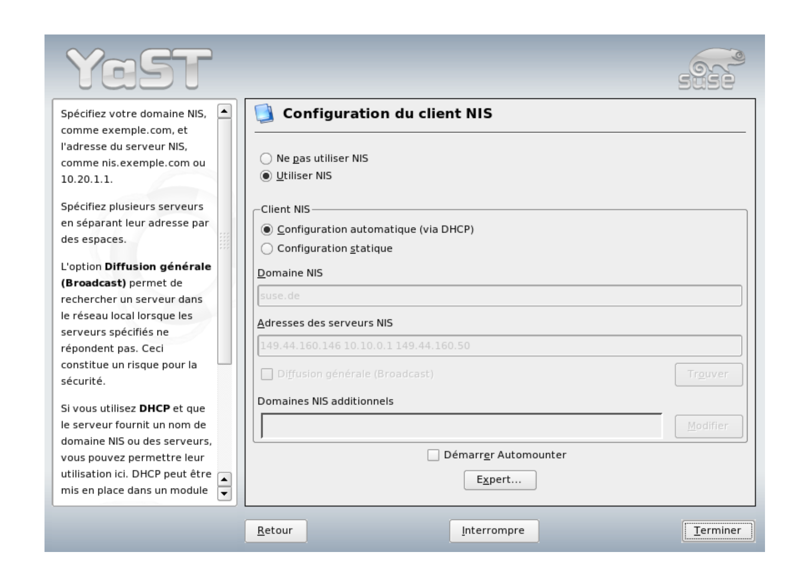


FIG. 25.4: *Saisie du domaine et de l'adresse du serveur NIS*

Partager des systèmes de fichiers avec NFS

Comme indiqué précédemment dans le chapitre 25 page 485, NFS travaille avec NIS dans le but de rendre un réseau transparent pour les utilisateurs. NFS permet de distribuer des systèmes de fichiers sur un réseau. Quel que soit le poste au sein du réseau sur lequel un utilisateur travaille, ce dernier retrouvera toujours le même environnement.

Tout comme NIS, NFS est un service asymétrique. Il y a des serveurs NFS et des clients NFS. Ces deux fonctions peuvent bien entendu coexister sur une même machine. Celle-ci proposera dans le même temps des systèmes de fichiers au réseau ("exportation") et montera des systèmes de fichiers appartenant à d'autres machines ("importation"). On utilise en règle générale des serveurs dotés d'une capacité disque importante, et ce seront leurs systèmes de fichiers qui seront montés par des clients.

Important

Nécessité d'un DNS

En principe, toutes les exportations peuvent être faites à l'aide des seules adresses IP. Cependant, afin d'éviter des délais, vous devriez avoir un système DNS en fonctionnement. Ceci est au moins nécessaire pour des raisons de journalisation parce que le démon mountd fait des consultations inverses.

Important

26.1 Importer des systèmes de fichiers avec YaST

Les utilisateurs qui y sont autorisés peuvent monter des répertoires NFS de serveurs NFS dans leur propre arborescence de fichiers. La méthode la plus simple pour ce faire consiste à utiliser le module 'client NFS' de YaST. Il suffit d'indiquer le nom d'hôte du serveur NFS, le répertoire à importer et le point de montage sous lequel il doit être monté sur le poste client. On peut fournir ces indications après avoir cliqué sur 'Ajouter' dans la première boîte de dialogue. Reportez-vous à la figure 26.1 de la présente page.



FIG. 26.1: *Configurer le client NFS avec YaST*

26.2 Importation manuelle de systèmes de fichiers

Il est très simple d'importer à la main des systèmes de fichiers à partir d'un serveur NFS. Pour ce faire, il suffit simplement que le redirecteur de ports (RPC portmapper) soit en service. Pour le démarrer, exécutez la commande `rcportmap start` en tant qu'utilisateur `root`. Lorsque cette condition est satisfaite, des systèmes de fichiers distants peuvent, s'ils sont exportés depuis les machines correspondantes, être montés dans le système de fichiers à l'aide de la commande `mount`, comme s'il s'agissait de disques locaux. La syntaxe est la suivante :

```
mount machine:chemin-distant chemin-local
```

Ainsi, la commande pour importer les répertoires personnels de la machine soleil est la suivante :

```
mount soleil:/home /home
```

26.3 Exportation de systèmes de fichiers avec YaST

Avec YaST, vous pouvez transformer un ordinateur de votre réseau en serveur NFS — un serveur qui exporte des répertoires et des fichiers pour tous les hôtes à qui on en donne l'accès. Ainsi, vous pouvez mettre des applications à la disposition de vos collaborateurs, sans qu'il soit nécessaire de les installer en local sur leurs machines. Pour installer un tel serveur, lancez YaST et choisissez 'Services réseau' → 'Serveur NFS'. Une boîte de dialogue comme celle illustrée dans la figure 26.2 page suivante) s'affiche alors.

Ensuite, cochez 'Démarrer le serveur NFS' et cliquez sur le bouton 'Suivant'. Saisissez dans la zone du haut les répertoires que vous souhaitez exporter et en-dessous les machines auxquelles vous souhaitez accorder l'accès. Cette boîte de dialogue est montrée dans la figure 26.3 page 495. On peut paramétrer quatre options pour chaque ordinateur : `single host`, `netgroups`, `wildcards` et `IP networks`. Pour plus de précisions sur ces options, veuillez vous reporter à `man exports`. Cliquez sur le bouton 'Terminer' pour achever la configuration.



FIG. 26.2: *Utilitaire de configuration du serveur NFS*

Important

Configuration automatique du pare-feu

Si un pare-feu (SuSEfirewall2) fonctionne sur votre système, YaST procède à sa configuration pour le serveur NFS dès que vous sélectionnez 'Ouvrir ports dans le pare-feu'. YaST active alors le service `nfs`.

Important

26.4 Exportation manuelle de systèmes de fichiers

Si vous préférez renoncer à vous faire assister par YaST, vous devez vous assurer que les services suivants sont démarrés sur le serveur NFS :

- Redirecteur de ports RPC (portmap)

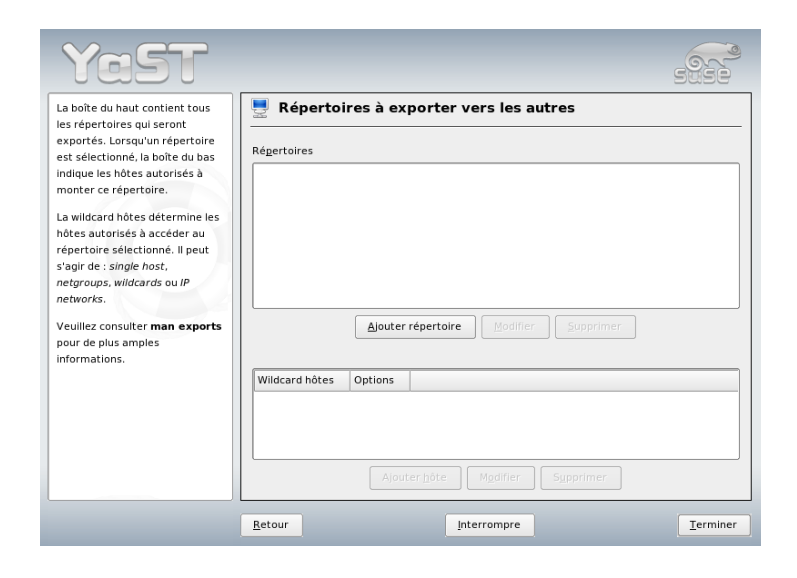


FIG. 26.3: *Configurer un serveur NFS avec YaST*

- Démon RPC de montage (rpc.mountd)
- Démon RPC NFS (rpc.nfsd)

Pour permettre aux scripts `/etc/init.d/portmap` et `/etc/init.d/nfsserver` de lancer ces services lors du démarrage du système, saisissez les commande `insserv /etc/init.d/nfsserver` et `insserv /etc/init.d/portmap`.

Lorsque ces démons ont été lancés, il vous reste à indiquer quels systèmes de fichiers doivent être exportés et vers quelles machines. Ces éléments sont définis dans le fichier `/etc/exports`.

Chaque répertoire à exporter utilise une ligne pour les informations relatives aux machines autorisées à y accéder et à leurs permissions. Tous les sous-répertoires d'un répertoire exporté sont aussi exportés automatiquement. Les machines autorisées sont habituellement désignées par leur nom (y compris le nom de domaine), mais on peut aussi utiliser des caractères joker comme `*` et `?` (qui fonctionnent de la même manière que dans l'interpréteur de commande Bash). Si aucun nom de machine n'est indiqué, toutes les machines sont autorisées à importer ce système de fichier avec les droits indiqués.

Vous pouvez paramétrer les permissions pour le système de fichier à exporter entre parenthèses après le nom de la machine. Les principales options sont montrées dans le tableau 26.1 de la présente page.

TAB. 26.1: *Droits d'accès aux répertoires exportés*

Option	Signification
`ro`	Le système de fichiers est exporté uniquement avec des droits en lecture (valeur par défaut).
`rw`	Le système de fichiers est exporté avec des droits en lecture/écriture.
`root_squash`	Grâce à cette option, l'utilisateur `root` d'une machine important des données ne possède sur ce système de fichiers aucun des spéciaux spécifiques à l'administrateur `root`. Ce résultat est obtenu en utilisant le numéro d'utilisateur `65534` pour les utilisateurs avec l'identifiant d'utilisateur `0`. Cet identifiant devrait être attribué à l'utilisateur `nobody` (valeur par défaut).
`no_root_squash`	Ne pas convertir l'identifiant `0` en identifiant `65534`; les privilèges de `root` sont donc conservés.
`link_relative`	Convertir les liens symboliques absolus (commençant par `/`) en une séquence correspondante de `../`. Cette option n'est utile que si le système de fichiers d'une machine a été monté dans sa totalité (valeur par défaut).
`link_absolute`	Laisser inchangés les liens symboliques.
`map_identity`	Le client utilise les mêmes numéros d'utilisateurs que sur le serveur (valeur par défaut).
`map_daemon`	Le client et le serveur utilisent des numéros d'utilisateurs distincts. Avec cette option, le programme nfsd va créer une table de conversion des numéros d'utilisateurs. Le démon ugidd est requis pour le bon fonctionnement de cette option.

Le fichier `exports` peut ressembler à l'exemple 26.1 de la présente page. Le fichier `/etc/exports` est lu par mountd et nfsd. Ainsi, lorsque ce fichier a été modifié, il est nécessaire de redémarrer mountd et nfsd afin de permettre à ces modifications d'être prises en compte. Pour ce faire, le plus simple est d'exécuter la commande `rcnfsserver restart`.

Example 26.1: */etc/exports*

```
#
# /etc/exports
#
/home            soleil(rw)   venus(rw)
/usr/X11         soleil(ro)   venus(ro)
/usr/lib/texmf   soleil(ro)   venus(rw)
/                terre(ro,root_squash)
/home/ftp        (ro)
# End of exports
```

DHCP

DHCP (”Dynamic Host Configuration Protocol“, protocole de configuration dynamique d’hôtes) sert à configurer un réseau de façon centralisée à partir d’un serveur. On n’a donc pas besoin de configurer chaque poste de travail séparément. Un hôte configuré avec le protocole DHCP ne dispose pas d’adresses statiques, mais se configure lui-même complètement en fonction des indications fournies par le serveur DHCP.

Il est en outre possible d'identifier chaque client à partir de l'adresse matérielle de sa carte réseau et de le configurer toujours de la même façon, ou alors d'attribuer dynamiquement à chaque ordinateur qui en demande des adresses puisées dans une réserve (en anglais, un pool) donnée. Dans ce cas, le serveur DHCP s'efforce d'attribuer toujours la même adresse à chaque hôte, lors de chaque requête (même après un long intervalle de temps). Cela ne fonctionne toutefois que tant qu'il y a plus d'adresses que d'hôtes dans le réseau.

Un administrateur système peut donc profiter immédiatement à deux égards du protocole DHCP. D'une part, il peut entreprendre des modifications d'adresses réseau ou de configuration, même en grand nombre, de manière confortable et centralisée dans le fichier de configuration du serveur DHCP. C'est bien plus pratique que de reconfigurer un grand nombre de stations de travail. D'autre part, il est très facile d'intégrer de nouveaux ordinateurs dans le réseau, dans la mesure où une adresse IP tirée de la réserve d'adresses leur est affectée. De plus, pour les ordinateurs portables qui sont régulièrement utilisés dans plusieurs réseaux différents, il est intéressant de pouvoir obtenir la configuration réseau appropriée à partir d'un serveur DHCP.

Outre l'adresse IP et le masque réseau, le nom de l'ordinateur et du domaine, la passerelle à utiliser et les adresses du serveur de noms sont communiqués au client. Par ailleurs, d'autres paramètres peuvent être configurés de manière centralisée, par exemple un serveur d'horloge auquel il est possible de demander l'heure actuelle ou même un serveur d'impression.

27.1 Configuration d'un serveur DHCP avec YaST

Lorsque le module démarre pour la première fois, YaST appelle un assistant de configuration en quatre étapes. À la fin de cet assistant, un serveur DHCP simple est prêt à fonctionner.

Choix de l'interface réseau Lors de la première étape, YaST détermine les interfaces réseau installées dans votre système. Choisissez dans la liste proposée celle pour laquelle le serveur DHCP devra être lancé et utilisez l'option 'Ouvrir le pare-feu pour l'interface sélectionnée' pour ouvrir le pare-feu sur cette interface. Reportez-vous à la figure 27.1 page suivante.

Paramètres globaux Vous pourrez configurer les informations que doit recevoir chaque client géré par ce serveur DHCP dans les zones de saisie. Ces

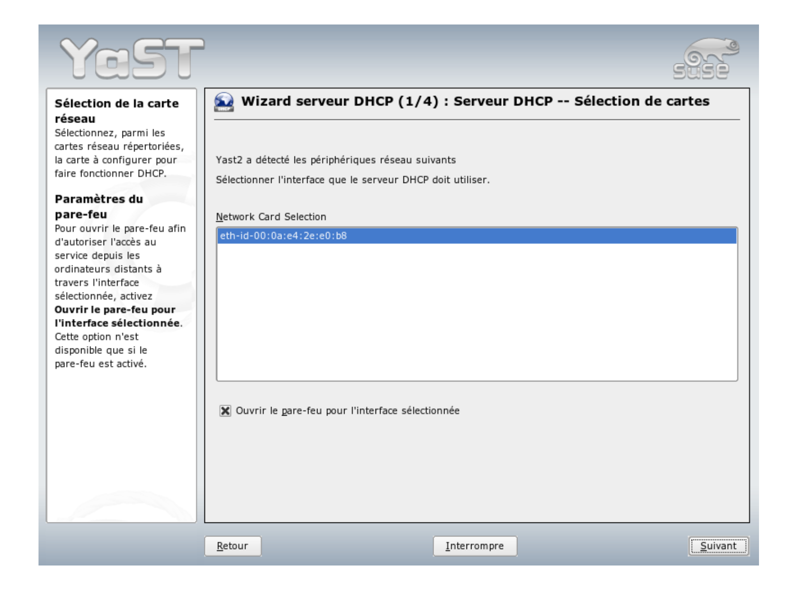


FIG. 27.1: *Serveur DHCP~: choix de l'interface réseau*

informations sont le nom du domaine, l'adresse d'un serveur d'horloge, l'adresse des serveurs de noms primaire et secondaire, l'adresse d'un serveur d'impression et celle d'un serveur WINS (pour l'intégration de clients Windows et Linux), ainsi que l'adresse de la passerelle et la durée du bail. Reportez-vous à la figure 27.2 page suivante.

DHCP dynamique Dans cette étape, on configure l'affectation IP dynamique aux clients connectés. Pour cela, définissez une plage d'adresses IP à partir de laquelle le serveur peut attribuer des adresses aux clients DHCP. Toutes les adresses doivent correspondre à un même masque réseau. Fixez aussi la durée du bail pendant laquelle le client peut garder une adresse sans avoir à faire de demande de prolongation. À titre facultatif, vous pouvez en outre établir la durée maximale du bail pendant laquelle une adresse IP reste réservée sur le serveur pour un client donné. Reportez-vous à la figure 27.3 page 503.

Fin de la configuration et choix du mode de démarrage
Une fois que vous en avez terminé avec la troisième étape de l'assistant de configuration, vous accédez à une dernière boîte de dialogue dans laquelle on définit comment le serveur DHCP doit être démarré. Vous pouvez y

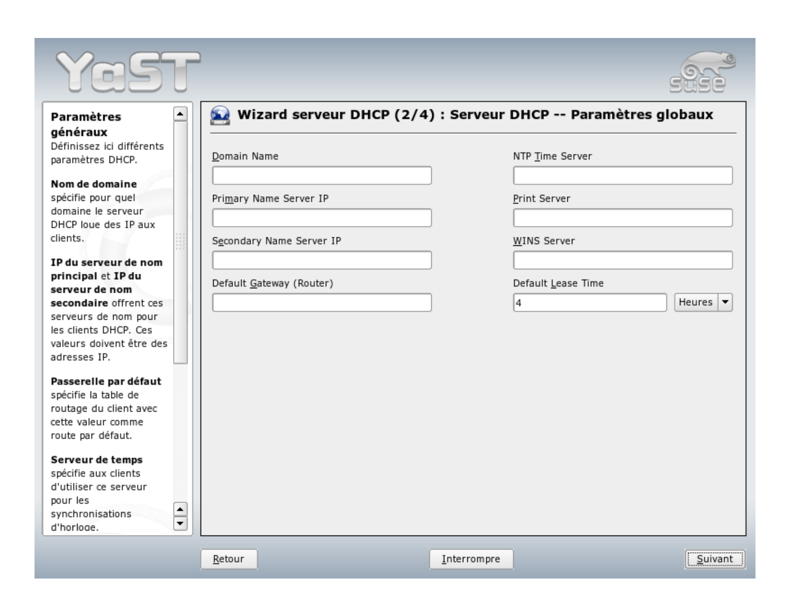


FIG. 27.2: *Serveur DHCP~: paramètres globaux*

indiquer si le serveur DHCP doit être lancé automatiquement au démarrage du système ou s'il doit être démarré manuellement à la demande (pour le tester, par exemple). Cliquez sur 'Terminer' pour achever la configuration du serveur. Reportez-vous à la figure 27.4 page 504).

27.2 Paquetages logiciels DHCP

SUSE LINUX comprend à la fois un serveur DHCP et des clients DHCP. Le serveur DHCP, dhcpd, est mis à disposition par l'Internet Software Consortium. Du côté du client, vous pouvez choisir entre deux programmes clients DHCP différents : dhclient (provenant également de l'ISC) et le démon client DHCP du paquetage `dhcpcd`.

Le démon dhcpcd installé par défaut avec SUSE LINUX est très facile à manipuler et démarre automatiquement lors du démarrage de l'ordinateur pour rechercher un serveur DHCP. Il n'a pas besoin de fichier de configuration pour faire son travail et fonctionne directement dans la majorité des configurations standard. Dans des situations plus compliquées, on peut recourir au programme dhclient

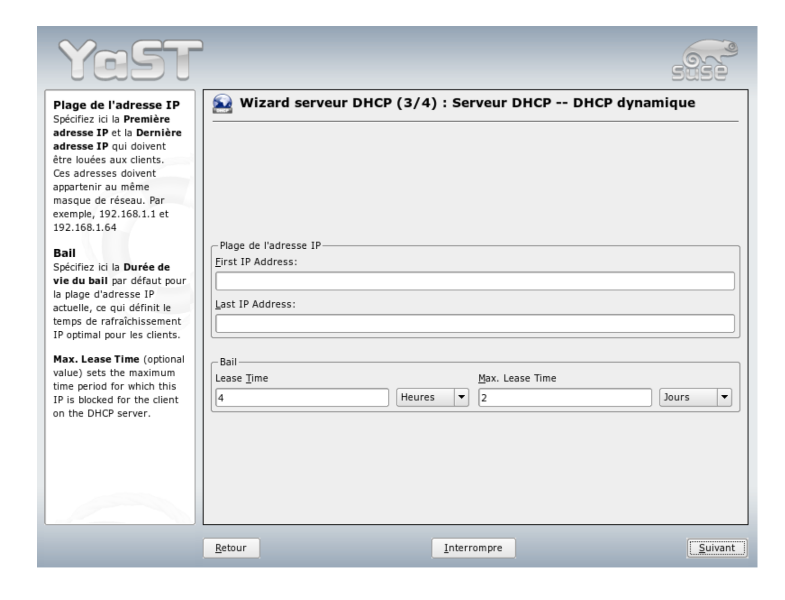


FIG. 27.3: *Serveur DHCP~:DHCP dynamique*

de l'ISC qui se paramètre avec le fichier de configuration `/etc/dhclient.conf`.

27.3 Le serveur DHCP dhcpd

Le démon de protocole de configuration des hôtes dynamique est au cœur de tout système DHCP. Ce serveur "loue" (to lease) des adresses et surveille leur utilisation en fonction de ce qui est indiqué dans le fichier de configuration `/etc/dhcpd.conf`. Grâce aux paramètres et aux valeurs définis dans ce fichier, l'administrateur système dispose d'un grand nombre de possibilités pour influencer comme il le souhaite le comportement du programme. Reportez-vous à l'exemple simple de fichier `/etc/dhcpcd.conf` de l'exemple 27.1 de la présente page.

Example 27.1: *Le fichier de configuration /etc/dhcpd.conf*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours
```

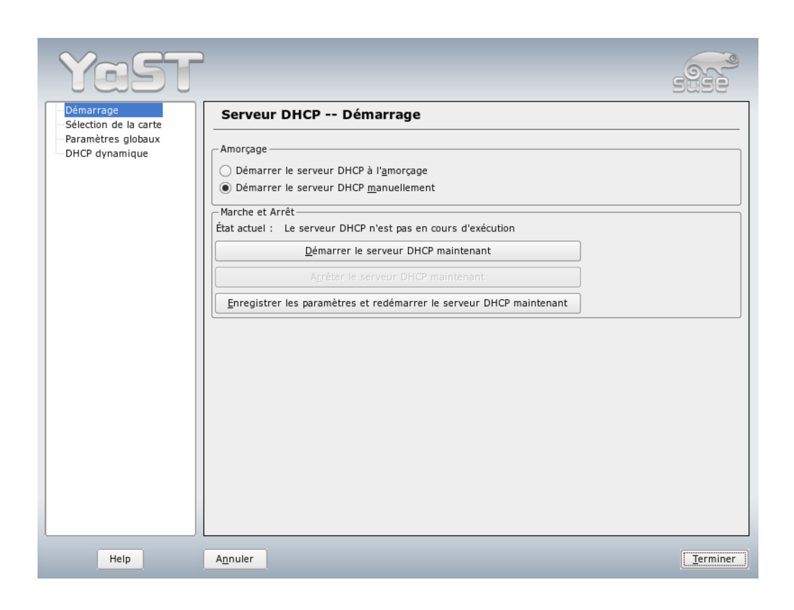


FIG. 27.4: *Serveur DHCP~: Démarrage*

```
option domain-name "kosmos.uni";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

Ce fichier de configuration simple est suffisant pour que le protocole DHCP puisse attribuer des adresses IP au réseau. Faites tout particulièrement attention aux points-virgules à la fin de chaque ligne : le démon dhcpd ne peut pas démarrer si vous les oubliez.

L'exemple de fichier ci-dessus peut se diviser en trois blocs. La première partie définit le nombre de secondes par défaut pendant lequel une adresse IP est

"louée" à un client qui le demande avant que ce dernier ne doive se préoccuper de demander une prolongation (`default-lease-time`, temps d'attribution par défaut). Est également indiquée ici la durée maximale pendant laquelle un ordinateur a le droit de conserver une adresse IP attribuée par le serveur DHCP sans avoir à demander de prolongation (`max-lease-time`, temps d'attribution maximal).

Le deuxième bloc définit de façon globale un certain nombre de paramètres réseau fondamentaux :

- L'option `option domain-name` (nom de domaine) définit le domaine par défaut de votre réseau.
- L'option `option domain-name-servers` (serveurs de noms de domaine) vous permet d'indiquer jusqu'à trois serveurs DNS à utiliser pour la résolution des adresses IP en noms d'hôtes (et réciproquement). Idéalement, il serait préférable qu'un serveur de noms soit déjà en service sur votre système ou dans votre réseau avant de paramétrer le serveur DHCP. Ce serveur de noms devrait aussi définir un nom d'hôte pour chaque adresse dynamique et réciproquement. Pour apprendre comment mettre en place un serveur de noms, reportez-vous au chapitre 24 page 463.
- L'option `option broadcast-address` (adresse de diffusion) définit l'adresse de diffusion que le client demandeur doit utiliser.
- L'option `option routers` (routeurs) indique au serveur où envoyer les paquets de données qui ne peuvent pas être distribués dans le réseau local (du fait de l'adresse de l'hôte source ou cible ainsi que des masques de sous-réseau indiqués). Dans la plupart des cas et en particulier pour les petits réseaux, ce routeur est également le point d'accès à l'Internet.
- L'option `option subnet-mask` (masque de sous-réseau) indique le masque réseau attribué au client.

Après ces réglages généraux, il faut encore définir un réseau à l'aide d'un masque de sous-réseau. Pour finir, il faut choisir un domaine d'adresses où le démon DHCP peut puiser pour attribuer des adresses aux clients qui en demandent. Dans l'exemple ci-dessus, toutes les adresses comprises entre `192.168.1.10` et `192.168.1.20` et entre `192.168.1.100` et `192.168.1.200` sont disponibles.

Après ces quelques lignes, vous devriez déjà être en mesure d'activer le démon DHCP avec la commande `rcdhcpd start`. Le serveur sera immédiatement prêt à être utilisé. Vous pouvez aussi vérifier rapidement la syntaxe du fichier de configuration avec `rcdhcpd check-syntax`. Si vous rencontrez un problème inattendu avec la configuration — le serveur s'interrompt avec une erreur et ne renvoie pas le message `done` au démarrage — vous trouverez la plupart du temps des informations sur l'incident dans le journal système central

/var/log/messages ou sur la console numéro 10 (Ctrl-Alt-F10).

Pour des raisons de sécurité, le démon DHCP démarre, sous SUSE LINUX, par défaut dans un environnement déraciné (chroot). Pour qu'il trouve les fichiers de configuration, vous devez également copier ces derniers dans le nouvel environnement. Il n'y a normalement pas besoin de s'en préoccuper, car cette opération s'effectue automatiquement avec la commande rcdhcpd start.

27.3.1 Clients avec adresses IP fixes

Comme déjà mentionné précédemment, le protocole DHCP permet aussi d'attribuer à un client, lors de chaque demande, une adresse donnée, bien précise. Ces attributions explicites d'adresses ont la priorité sur les adresses dynamiques extraites de la réserve. Contrairement aux adresses dynamiques, les informations d'adresses fixes n'expirent pas comme c'est le cas lorsqu'il n'y a plus assez d'adresses disponibles et qu'une nouvelle répartition est nécessaire.

Pour identifier un client défini à l'aide d'une adresse *statique*, dhcpd utilise l'adresse matérielle qui est un numéro unique dont dispose chaque périphérique réseau, défini de manière fixe et composé de six paires d'octets (par exemple, 00:00:45:12:EE:F4). Si le fichier de configuration de l'exemple 27.1 page 503 est complété par une définition semblable à celle de l'exemple 27.2 de la présente page, dhcpd enverra quoi qu'il arrive les mêmes données au client concerné.

Example 27.2: *Complément au fichier de configuration*

```
host terre {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

On indique tout d'abord le nom du client à définir (host ⟨*nom de machine*⟩, ici terre) et, sur la ligne suivante, son adresse MAC. Sur les ordinateurs sous Linux, cette adresse peut être déterminée à l'aide de la commande ifstatus suivie du périphérique réseau (par exemple eth0). Vous devez, le cas échéant, d'abord activer la carte : ifup eth0. Vous obtenez alors un affichage de la forme :

```
link/ether 00:00:45:12:EE:F4
```

Dans notre exemple, le client dont la carte réseau possède l'adresse MAC `00:00:45:12:EE:F4` se verra donc attribuer l'adresse IP `192.168.1.21` ainsi que le nom d'hôte terre. De nos jours, le matériel utilisé est en général de type `ethernet`, même si la technologie `token-ring`, fréquente notamment sur les systèmes IBM, est également prise en charge.

27.3.2 Particularités propres à SUSE LINUX

Pour des raisons de sécurité, la version pour SUSE du serveur DHCP publié par l'ISC contient le correctif non-root/chroot d'Ari Edelkind. Ainsi, dhcpd s'exécute en tant qu'utilisateur `nobody` et dans un environnement déraciné (`/var/lib/dhcp`). Le fichier de configuration `dhcp.conf` doit pour cela se trouver dans `/var/lib/dhcp/etc` ; il y sera automatiquement copié par le script d'initialisation lors du démarrage.

On contrôle le comportement du serveur pour cette fonctionnalité grâce au fichier `/etc/sysconfig/dhcpd`. Pour démarrer dhcpd sans environnement déraciné, donnez la valeur "no" à la variable `DHCPD_RUN_CHROOTED` du fichier `/etc/sysconfig/dhcpd`.

Pour que dhcpd puisse également résoudre les noms d'hôtes dans l'environnement déraciné, il faut copier quelques fichiers de configuration supplémentaires. Il s'agit de :

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Ces fichiers sont copiés dans `/var/lib/dhcp/etc/` lorsque le script d'initialisation du système est lancé. Veillez à ce que les modifications soient propagées s'ils sont modifiés dynamiquement par des scripts comme `/etc/ppp/ip-up`. En revanche, il n'y a aura aucun problème si l'on utilise uniquement des adresses IP dans le fichier de configuration à la place des noms d'hôtes.

Si, dans votre configuration, vous devez copier d'autres fichiers dans l'environnement déraciné, indiquez-les avec le paramètre `DHCPD_CONF_INCLUDE_FILES` dans le fichier `etc/sysconfig/dhcpd`. Pour que le démon dhcp puisse continuer à enregistrer le journal à partir de l'environnement déraciné même si le démon syslog est redémarré, ajoutez le paramètre `"-a /var/lib/dhcp/dev/log"` à la variable `SYSLOGD_PARAMS` du fichier `/etc/sysconfig/syslog`.

27.4 Pour plus d'informations

Vous trouverez des informations complémentaires à propos de DHCP sur le site de l'*Internet Software Consortium* (`http://www.isc.org/products/DHCP/`, en anglais). Vous trouverez également des informations dans les pages de manuel de `dhcpd`, `dhcpd.conf`, `dhcpd.leases` et `dhcp-options`.

Synchronisation temporelle avec xntp

Le mécanisme NTP (Network Time Protocol) est un protocole de synchronisation du temps d'un système via le réseau. Tout d'abord, un ordinateur peut obtenir l'heure de tout serveur qui est une source de temps fiable. Par ailleurs, un ordinateur peut agir lui-même comme source de temps pour d'autres ordinateurs du réseau. L'objectif est double : maintenir le temps absolu et la synchronisation de l'horloge système de tous les ordinateurs d'un réseau.

Dans de nombreuses situations, il est important de maintenir l'heure exact dans le système. L'horloge matérielle intégrée (BIOS) n'est pas toujours adaptée aux besoins d'applications telles que des bases de données. La correction manuelle du temps du système causerait de sérieux problèmes car un retardement de l'horloge, par exemple, pourrait provoquer des dysfonctionnements des applications critiques. Dans un réseau, il est généralement nécessaire de synchroniser l'heure de tous les ordinateurs mais l'ajustement manuel n'est pas très judicieux. xntp offre un mécanisme qui résout ces problèmes. Il ajuste continuellement l'heure du système à l'aide de serveurs de temps fiables du réseau. En outre, il permet la mise en place d'étalons de temps locaux tels que des horloges à fréquence radio.

28.1 Configuration de xntp dans le réseau

Le programme xntp est préréglé de manière à utiliser l'horloge système locale comme référence temporelle. Cependant, l'utilisation de l'horloge (BIOS) ne sert que comme solution de rechange lorsqu'aucune source de temps plus précise n'est disponible. Le plus simple pour utiliser un serveur de temps sur le réseau est de spécifier des paramètres "server". Dans le cas où un serveur de temps nommé, par exemple, `ntp.example.com`, est joignable dans le réseau, ajoutez son nom dans le fichier `/etc/ntp.conf` en entrant la ligne `server ntp.example.com`.

Il est facile d'ajouter des serveurs de temps en ajoutant de nouvelles lignes utilisant le mot-clé "server". Après avoir été lancé à l'aide de la commande `rcxntpd start`, le démon xntpd a besoin d'environ une heure jusqu'à ce que l'horloge se stabilise. Le fichier de dérive temporelle (fichier "drift") est alors créé afin de pouvoir corriger l'horloge système locale. Le fichier "drift" permet de connaître le décalage de l'horloge systèmeau démarrage de la machine. La correction est alors immédiatement activée, ce qui permet d'offrir une plus grande stabilité de l'horloge système.

Le mécanisme NTP peut être utilisé de deux façons en tant que client : Tout d'abord, le client peut obtenir l'heure d'un serveur connu à intervalles réguliers. Si les clients sont nombreux, cette approche peut causer une charge très importante du serveur. Par ailleurs, le client peut attendre une multidiffusion NTP envoyée dans le réseau par des serveurs de temps multidiffusion. Cette méthode présente un inconvénient : la qualité du serveur est inconnue et un serveur qui envoie de mauvaises informations peut provoquer des problèmes sérieux.

Si vous obtenez le temps au moyen d'une diffusion, vous n'avez pas besoin de connaître le nom du serveur. Dans ce cas, vous pouvez également entrer la ligne

broadcastclient dans le fichier de configuration /etc/ntp.conf. Pour utiliser exclusivement un ou plusieurs serveurs de temps, entrez leur nom dans la ligne débutant avec servers.

28.2 Mise en place d'un étalon de temps local

L'application xntp comporte également des pilotes permettant de se connecter à des étalons de temps locaux. Vous trouverez la liste des horloges prises en charge dans le paquetage xntp-doc dans le fichier /usr/share/doc/packages/xntp-doc/html/refclock.htm. Chaque pilote est identifié par un numéro. La configuration de xntp à proprement parler est assurée à l'aide de pseudo adresses IP. Les horloges sont déclarées dans le fichier /etc/ntp.conf comme s'il s'agissait d'horloges disponibles sur le réseau. Elles reçoivent pour cela des adresses IP particulières sur le modèle suivant : 127.127.t.u. Ici, t signifie le type de l'horloge et détermine quel pilote est utilisé tandis que u signifie unité et détermine l'interface utilisée.

Les différents pilotes ont normalement des paramètres spéciaux chargés de décrire plus en détail la configuration. Vous trouverez, dans le fichier /usr/share/doc/packages/xntp-doc/html/driverNN.htm (où NN représente le numéro du pilote), des informations relatives au type d'horloge en question. Pour l'horloge de "type 8", par exemple, il est nécessaire d'indiquer un mode supplémentaire chargé de spécifier l'horloge plus exactement. Ainsi, le "module récepteur Conrad DCF77" utilise le "mode 5". Pour que cette horloge soit prise comme référence par xntp, vous pouvez également indiquer le mot-clé prefer. La ligne server complète d'un "module récepteur Conrad DCF77" est donc :

```
server 127.127.8.0 mode 5 prefer
```

D'autres horloges sont conçues sur le même schéma. La documentation sur xntp peut être consultée dans le répertoire /usr/share/doc/packages/xntp-doc/html, après l'installation du paquetage xntp-doc. Dans le fichier /usr/share/doc/packages/xntp-doc/html/refclock.htm, vous trouverez des liens vers les pages du pilote qui décrivent les paramètres du pilote.

28.3 Configuration d'un client NTP avec YaST

Outre la configuration manuelle de xntp décrite précédemment, SUSE LINUX prend également en charge la configuration d'un client NTP par YaST. Vous disposez d'une configuration rapide et simple ou d'une configuration complexe. Celles-ci sont décrites dans les sections ci-après.

28.3.1 Configuration rapide du client NTP

La configuration simple d'un client NTP se fait en deux dialogues. Dans le premier dialogue, définissez le mode de démarrage de xntpd et le serveur à interroger. Pour le démarrer automatiquement lors de l'amorçage du système, cliquez sur le bouton radio 'Lors de l'amorçage'. Pour déterminer un serveur de temps adapté pour votre réseau, cliquez sur 'Sélectionner' et entrez dans le second dialogue afin de sélectionner le serveur de temps pour votre réseau.

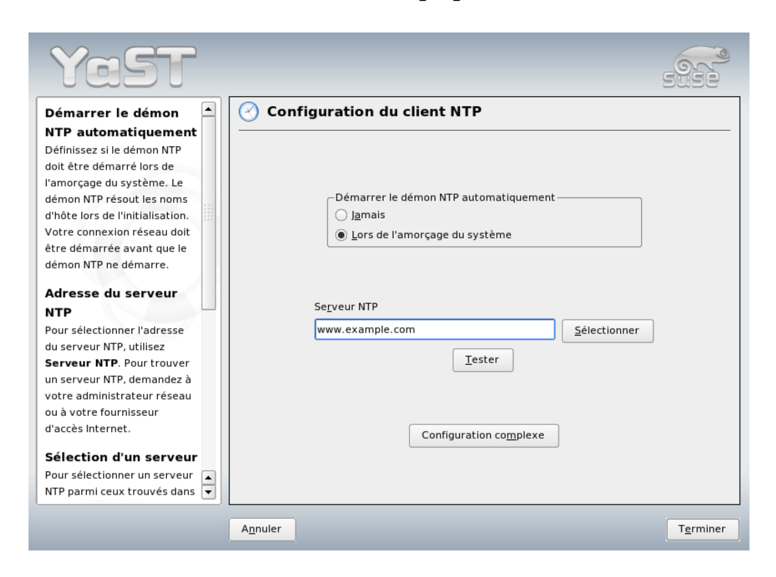


FIG. 28.1: *YaST~: configuration du client NTP*

Dans le dialogue détaillé pour le choix du serveur, définissez d'abord si vous souhaitez utiliser un serveur de votre propre réseau ou un serveur de temps d'Internet de votre zone horaire ('Serveur NTP public') pour la synchronisation du temps. Dans le cas d'un serveur de temps local, cliquez sur 'Recherche' pour procéder à une requête SLP des serveurs de temps disponibles dans votre réseau. Dans la liste des résultats, sélectionnez le serveur adéquat et quittez le dialogue avec 'OK'. Pour un serveur de temps public, sélectionnez votre pays (zone horaire) et le serveur qui vous convient dans 'Serveur NTP public'. Quittez le dialogue avec 'OK'. Quittez la configuration avec 'Terminer' une fois que vous avez vérifié la disponibilité du serveur sélectionné à l'aide de 'Test'.

28.3.2 Configuration complexe du client NTP

Vous pouvez accéder à la configuration complexe du client NTP sous 'Configuration complexe' dans le dialogue principal du module 'client NTP' tel que dans la figure 28.1 page précédente une fois que vous avez le mode démarrage tel que décrit dans la configuration rapide.

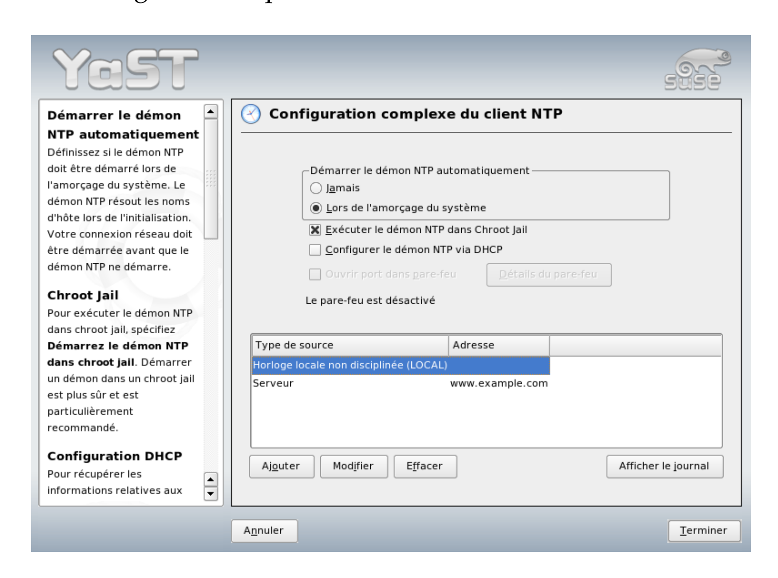


FIG. 28.2: *YaST~: configuration complexe du client NTP*

Dans le dialogue 'configuration complexe du client NTP', définissez si xntpd doit être démarré dans un chroot jail. Cela augmente la sécurité dans le cas d'une attaque à travers xntpd, l'attaquant n'ayant alors pas la possibilité de compromettre le système entier. En outre, vous pouvez, avec 'Configurer le démon NTP via DHCP', configurer le client NTP de façon à ce qu'il soit informé par DHCP de la liste des serveurs NTP disponibles dans votre réseau.

Dans la partie inférieure de la fenêtre de dialogue, les sources d'information du client sont répertoriées. Vous pouvez modifier cette liste avec 'Ajouter', 'Modifier' et 'Effacer'. Avec 'Avancé', vous avez la possibilité de consulter les fichiers de journalisation de votre client ou d'accorder le pare-feu à la configuration du client NTP.

Pour ajouter une nouvelle source de synchronisation du temps, cliquez sur 'Ajouter'. Dans le dialogue suivant, sélectionnez le type de la source avec laquelle la synchronisation du temps doit se faire. Les options suivantes sont disponibles :

Serveur Dans le dialogue suivant, vous pouvez sélectionner le serveur NTP (comme décrit dans la section 28.3.1 page 512) et vous pouvez activer l'option 'Utiliser pour synchronisation initiale' afin de procéder à une synchronisation du temps entre serveur et client au moment de l'amorçage. Dans un autre champ de saisie, vous pouvez compléter des options supplémentaires pour xntpd. Vous trouverez des informations détaillées à ce sujet sous `/usr/share/doc/packages/xntp-doc`.

Pair Un pair est une machine avec laquelle une relation symétrique est établie : elle agit à la fois en tant que serveur de temps et en tant que client. Si la synchronisation se fait avec un pair dans le même réseau plutôt qu'avec un serveur, saisissez l'adresse de ce système. Le dialogue qui suit est identique à celui du 'Serveur'.

Horloge radio Si vous utilisez une horloge radio dans votre système et souhaitez l'utiliser pour la synchronisation du temps, entrez dans ce dialogue le type de l'horloge, le numéro du périphérique, le nom du périphérique et les autres options. Avec 'Calibration du pilote', procédez à la configuration fine des pilotes correspondants. Vous trouverez des informations détaillées sur l'utilisation d'une horloge radio locale sous `/usr/share/doc/packages/xntp-doc/html/refclock.htm`.

Diffusion générale (broadcasting) Les informations et requêtes de temps peuvent également être transmises dans le réseau par diffusion générale. Entrez dans ce dialogue les adresses auxquelles de telles diffusions générales doivent être envoyées. N'activez la diffusion générale que si vous avez une source de temps fiable telle qu'une horloge radio.

Accepter des paquets de diffusion générale
Si votre client doit recevoir ses informations par diffusion générale, entrez dans ce dialogue de quelles adresses les paquets correspondants doivent être acceptés.

LDAP – un service d'annuaire

Le protocole léger d'accès aux annuaires (LDAP, en anglais Lightweight Directory Access Protocol) est un ensemble de protocoles conçu pour maintenir et accéder à des annuaires d'informations. LDAP peut être utilisé pour de nombreux objectifs comme la gestion des utilisateurs et des groupes, la gestion de la configuration système ou la gestion des adresses. Ce chapitre propose une compréhension des bases du fonctionnement de LDAP et vous explique comment gérer des données LDAP avec YaST.

Il est fondamental, dans un environnement de travail en réseau, de pouvoir disposer rapidement et de manière structurée de diverses informations importantes. Ce problème est résolu par un service d'annuaire permettant, comme les pages jaunes (en anglais Yellow Pages) du monde réel, d'accéder rapidement et de façon structurée aux informations recherchées.

Idéalement, il existe un serveur central gérant les données dans un annuaire et les partageant avec tous les clients dans le réseau à l'aide d'un protocole donné. Les données doivent être structurées de manière à permettre à la plus large gamme d'applications possible d'y accéder. Ainsi, il n'est pas nécessaire que chaque application d'agenda ou chaque client de messagerie gère ses propres bases de données—il suffit que chacun puisse accéder au référentiel commun. Ce mode de gestion réduit de manière appréciable la charge de gestion pour les informations concernées. Le fait d'utiliser un protocole ouvert et standardisé comme LDAP garantit qu'autant d'applications clientes que possible peuvent accéder à ces informations.

Dans ce contexte, un annuaire est une sorte de base de données optimisée de manière à permettre une consultation et des recherches rapides et précises :

- Afin de permettre des accès en lecture nombreux (simultanés), on restreint l'accès en écriture à un nombre d'actualisations réduit, faites par l'administrateur. Les bases de données classiques sont optimisées afin de pouvoir traiter très rapidement un volume de données considérable.
- Les accès en écriture ne doivent s'effectuer que de manière très limitée. C'est la raison pour laquelle on gère dans un service d'annuaire des informations *statiques*. En général, les données contenues dans une base de données classique se modifient très fréquemment (données *dynamiques*). Les numéros de téléphone dans un annuaire du personnel ont un rythme de modification beaucoup moins élevé que les chiffres traités par la comptabilité par exemple.
- Lorsque des données statiques sont gérées, il est très rare que les enregistrements existants soient mis à jour. Lorsque l'on gère des données dynamiques, en particulier pour des enregistrements tels que des comptes bancaires ou pour de la comptabilité, la cohérence des données est primordiale. Ainsi, si l'on doit débiter une somme à un endroit donné pour la créditer à un autre endroit, les deux opérations doivent être exécutées en même temps, dans le cadre d'une seule *transaction*, afin de s'assurer que les données restent équilibrées. Les bases de données prennent en charge ce type de transactions, contrairement aux annuaires. Des incohérences temporaires dans les données sont tout à fait acceptables dans le cas des annuaires.

De par sa conception, un service d'annuaire tel que LDAP n'est pas prévu pour prendre en charge des mécanismes complexes de mises à jour ou de requêtes.

Toutes les applications accédant à ce service doivent bénéficier d'un accès qui soit le plus aisé et le plus rapide possible.

Il y a eu et il y a encore un grand nombre de services d'annuaire, et pas uniquement dans le monde Unix : NDS de Novell, ADS de Microsoft, Street Talk de Banyan ainsi que la norme OSI X.500. Le protocole LDAP était initialement conçu comme une variante allégée du protocole DAP (ou Directory Access Protocol), qui avait été conçu pour l'accès X.500. La norme X.500 régit l'organisation hiérarchique des enregistrements d'annuaire.

LDAP, qui a perdu quelques fonctions du protocole DAP, est multi-plate-forme et consomme peu de ressources, sans qu'il soit nécessaire de renoncer aux hiérarchies d'enregistrements définies dans X.500. L'utilisation de TCP/IP simplifie considérablement la réalisation d'interfaces entre les applications et le service LDAP.

Entre temps, le service LDAP a continué à se développer et est de plus en plus fréquemment utilisé comme solution à part entière sans prise en charge de X.500. Avec LDAPv3 (la version du protocole du paquetage `openldap2`), LDAP prend en charge les *redirections* (en anglais, referrals) à l'aide desquels on peut créer des bases de données réparties. Autre nouveauté : la prise en charge de SASL (Simple Authentication and Security Layer), une couche d'authentification et de sécurité.

LDAP ne se limite pas à l'interrogation de serveurs X.500, comme cela était initialement prévu. On utilise également le programme slapd, un serveur open source permettant d'enregistrer dans une base de données locale des informations sur des objets. Ce programme est complété par le programme slurpd, chargé de la réplication de plusieurs serveurs LDAP.

Le paquetage `openldap2` comporte :

slapd Un serveur LDAPv3 unique gérant des informations sur des objets dans une base de données de type BerkeleyDB.

slurpd Ce programme permet de répliquer des modifications apportées aux données du serveur LDAP local sur d'autres serveurs LDAP installés sur le réseau.

des outils supplémentaires de gestion système
`slapcat`, `slapadd`, `slapindex`

29.1 LDAP par rapport à NIS

L'administrateur système Unix utilise traditionnellement le service NIS pour la résolution de noms et pour le partage des données au sein du réseau. Les données de configuration des fichiers `/etc` et des répertoires `group`, `hosts`, `mail`,

`netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` et `services` sont distribués par les clients dans tout le réseau. S'agissant de simples fichiers de texte, la maintenance de ces fichiers ne pose pas de difficulté particulière. Toutefois, lorsque le volume de données est important, ils s'avèrent peu pratiques à gérer en raison de l'absence de structuration. Le service NIS étant uniquement conçu pour les plate-formes Unix, il est impossible de l'utiliser pour une gestion centrale des données dans un réseau hétérogène.

À la différence du service NIS, le domaine d'utilisation du service LDAP ne se borne pas aux réseaux Unix. Les serveurs Windows (à partir de la version 2000) prennent en charge le service d'annuaire LDAP. Novell propose quant à lui également un service LDAP. Ce dernier ne se borne pas aux domaines d'utilisation précités.

Le principe de LDAP peut être appliqué à n'importe quel type de structures de données nécessitant une gestion centralisée. Voici quelques exemples d'applications :

- Utilisation à la place d'un service NIS
- Routage de messagerie (postfix, sendmail)
- Carnets d'adresses pour des clients de messagerie tels que Mozilla, Evolution et Outlook
- Gestion de descriptions de zones pour un serveur de nom BIND9

Cette énumération pourrait se poursuivre, du fait de l'extensibilité de LDAP, à la différence de NIS. La structure hiérarchique clairement définie des données apporte une aide appréciable dans la gestion des volumes de données très importants, grâce aux facilités de recherche qu'elle autorise.

29.2 Structure d'une arborescence d'annuaire LDAP

Un annuaire LDAP utilise une structure arborescente. Tous les enregistrements (ou objets) de l'annuaire ont une position définie au sein de cette hiérarchie. Celle-ci est connue sous le nom d'*arbre d'informations d'annuaire* (Directory Information Tree ou DIT. Le chemin complet vers l'enregistrement souhaité permettant de l'identifier de manière unique est le *nom distingué* (Distinguished name) ou DN. Les différents nœuds du chemin vers cet enregistrement sont des *noms distingués relatifs* (Relative Distinguished Name) ou RDN. Les objets peuvent généralement être rattachés à deux types distincts :

Conteneur Ces objets peuvent contenir à leur tour d'autres objets. Ces classes d'objet sont `Root` (élément racine de l'arborescence qui n'existe pas réellement), `c` (pays, de l'anglais country), `ou` (unité d'organisation, de l'anglais organizational unit) et `dc` (composant de domaine, de l'anglais domain component). Ce type d'objets peut également être comparé aux répertoires (dossiers) du système de fichiers.

Feuille Ces objets sont localisés à l'extrémité d'une branche. Aucun autre objet ne leur est rattaché. Les exemples sont `person`, `InetOrgPerson` et `groupofNames`.

Un élément racine `root` se trouve à la tête de l'arborescence. Vous pouvez lui rattacher au niveau suivant au choix `c` (pays), `dc` (composant de domaine) ou `o` (organisation). Les relations à l'intérieur d'une arborescence LDAP sont illustrées par l'exemple ci-après illustré dans la figure 29.1 de la présente page.

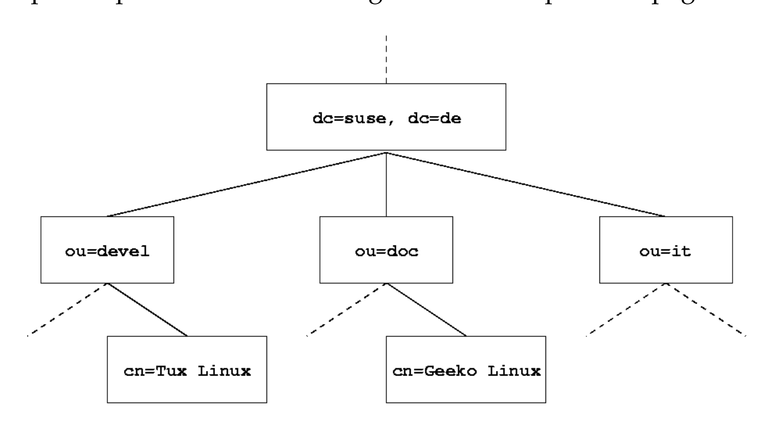


FIG. 29.1: *Structure d'un annuaire LDAP*

L'illustration décrit un *Directory Information Tree* fictif. Elle représente les enregistrements (entries) sur trois niveaux. Chaque enregistrement est représenté dans l'illustration par un rectangle. Le *nom distingué* (Distinguished Name) complet de l'employé de SUSE fictif, `Geeko Linux` est en l'occurrence `cn=Geeko Linux,ou=doc,dc=suse,dc=de`. Il est formé en ajoutant le RDN `cn=Geeko Linux` au DN de l'enregistrement précédent `ou=doc,dc=suse,dc=de`.

Les types d'objets qu'on a décidé a priori d'enregistrer dans le DIT sont décrits par un *schéma*. Le type correspondant à un objet est défini par la *classe d'objet*. Celle-ci définit les attributs qui doivent ou qui peuvent être rattachés à l'objet

concerné. Par conséquent, un schéma doit comporter les définitions de toutes les classes d'objets ainsi que les attributs utilisés dans le scénario de mise en œuvre souhaité. Il existe un certain nombre de schémas utilisables de manière générale (voir RFC 2252 et 2256). Il est également possible, toutefois, de créer des schémas personnalisés ou d'en utiliser plusieurs sur une base de complémentarité, lorsque cela est requis par l'environnement dans lequel le serveur LDAP doit être mis en œuvre.

Le tableau 29.1 de la présente page donne un aperçu des classes d'objet de `core.schema` et de `inetorgperson.schema` utilisées dans l'exemple, y compris les attributs obligatoires requis et les valeurs d'attributs admises.

TAB. 29.1: *Classes d'objets et attributs fréquemment utilisés*

Classe d'objet	Signification	Exemple d'enregistrement	Attributs requis
dcObject	*domainComponent* (éléments constituant le nom du domaine)	suse	dc
organizationalUnit	*organizationalUnit* (unité d'organisation)	doc	ou
inetOrgPerson	*inetOrgPerson* (données nominatives pour intranet ou Internet)	Geeko Linux	sn et cn

L'exemple 29.1 de la présente page montre un extrait d'une instruction de schéma avec des explications.

Example 29.1: *Extrait de schema.core (les lignes ont été numérotées pour plus de clarté)*

```
...
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2        DESC 'RFC2256: organizational unit this object belongs to'
#3        SUP name )
...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5    DESC 'RFC2256: an organizational unit'
```

```
#6        SUP top STRUCTURAL
#7    MUST ou
#8        MAY (userPassword $ searchGuide $ seeAlso $ businessCategory $
              x121Address $ registeredAddress $ destinationIndicator $
              preferredDeliveryMethod $ telexNumber $
              teletexTerminalIdentifier $ telephoneNumber $
              internationaliSDNNumber $ facsimileTelephoneNumber $
              street $ postOfficeBox $ postalCode $ postalAddress $
              physicalDeliveryOfficeName $ st $ l $ description) )
...
```

L'exemple présente le type d'attribut `organizationalUnitName` et la classe d'objet correspondante `organizationalUnit`. La ligne 1 énumère le nom de l'attribut, son OID (identificateur d'objet, Object Identifier) (numérique) ainsi que la forme abrégée de l'attribut.

La ligne 2 introduit avec `DESC` une brève description de l'attribut. Le RFC correspondant sur lequel est basée la définition y est également mentionné. `SUP` à la ligne 3 renvoie à un type d'attribut hiérarchiquement de niveau supérieur auquel cet attribut est rattaché.

La définition de la classe d'objet `organizationalUnit` commence à la ligne 4 par la définition d'attribut avec un OID et le nom de la classe d'objet. La ligne 5 comporte une brève description de la classe d'objet. À la ligne 6, l'enregistrement `SUP top` spécifie que cette classe d'objet n'est la sous-classe d'aucune classe d'objet. La ligne 7, commençant par `MUST`, énumère tous les types d'objets *obligatoirement* présents dans un objet de type `organizationalUnit`. La ligne 8 énumère, après `MAY`, tous les types d'attributs pouvant être utilisés dans cette classe d'objet.

Vous trouverez une excellente introduction à l'utilisation des schémas dans la documentation OpenLDAP. Lorsque OpenLDAP est installé, vous la trouverez à l'emplacement `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

29.3 Configuration d'un serveur avec slapd.conf

Lorsque le système est installé, `/etc/openldap/slapd.conf` est disponible comme fichier de configuration complet pour le serveur LDAP. Vous trouverez ci-après une description des différents enregistrements, précisant les ajustements à

apporter. Les lignes commençant par un # sont inactives. Pour activer ces lignes, il vous suffit de supprimer ce caractère de commentaire de la ligne choisie.

29.3.1 Instructions globales dans slapd.conf

Example 29.2: *slapd.conf : Instruction Include pour les schémas*

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/inetorgperson.schema
```

Cette première instruction de `slapd.conf`, montrée dans l'exemple 29.2 de la présente page,indique quel schéma est utilisé pour l'organisation de votre annuaire LDAP. La ligne `core.schema` est toujours requise. Dans le cas où vous auriez besoin de schémas supplémentaires, ajoutez-les à la suite de cette instruction (l'exemple ajouté ici est `inetorgperson.schema`). Vous pourrez trouver d'autres schémas disponibles dans le répertoire `/etc/openldap/schema/`. Si vous voulez remplacer le service NIS par un service LDAP équivalent, mentionnez à cet endroit les schémas `cosine.schema` et `rfc2307bis.schema`. Pour plus d'informations, reportez-vous à la documentation de OpenLDAP fournie.

Example 29.3: *slapd.conf : pidfile et argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Ces deux fichiers contiennent l'identificateur de processus (PID, de l'anglais process id) ainsi que différents arguments utilisés pour le lancement du processus `slapd`. Aucune modification n'est nécessaire ici.

Example 29.4: *slapd.conf : Contrôle d'accès*

```
# Sample Access Control
#       Allow read access of root DSE
#       Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
#
access to dn="" by * read
```

```
access to *
       by self write
       by users read
       by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

L'exemple 29.4 page précédente est l'extrait de code du fichier `slapd.conf` qui paramètre le contrôle d'accès à l'annuaire LDAP sur le serveur. Les paramètres qui sont définis dans la section globale du fichier `slapd.conf` s'appliquent tant qu'aucune règle d'accès particulière distincte n'a été établie dans la section propre à la base de données. Ces règles ont priorité sur les déclarations globales. Dans la configuration présentée, tous les utilisateurs ont un accès en lecture à l'annuaire, mais l'administrateur (`rootdn`) est le seul à pouvoir écrire dans cet annuaire. La définition des privilèges d'accès sous LDAP est un processus extrêmement complexe. Les astuces qui suivent peuvent aider :

- Chaque règle d'accès a la structure suivante :

  ```
  access to <quoi> by <qui> <accès>
  ```

- ⟨*quoi*⟩ représente l'objet ou l'attribut auquel vous accordez l'accès. Vous pouvez utiliser des règles séparées pour protéger de manière explicite différentes branches de l'arborescence ou des expressions rationnelles pour traiter des zones complètes de l'arborescence à l'aide d'une règle. `slapd` évalue toutes les règles dans l'ordre dans lequel elles ont été introduites dans le fichier de configuration. Vous devez donc toujours placer les règles génériques à la suite des règles plus spécifiques. `slapd` applique la première règle qui s'applique et toutes les lignes suivantes sont ignorées.
- Le paramètre ⟨*qui*⟩ détermine qui peut accéder aux domaines définis avec ⟨*quoi*⟩. Vous pouvez, ici aussi, utiliser des expressions rationnelles.`slapd` interrompt l'évaluation de `qui` après le première concordance, les règles spécifiques doivent donc être listées avant les règles générales. Les enregistrements énumérés dans le tableau 29.2 page suivante sont possibles.

TAB. 29.2: *Groupes d'utilisateurs et leurs droits d'accès*

Descripteur	Portée
`*`	tous les utilisateurs sans exception
`anonymous`	utilisateurs non authentifiés ("anonymes")
`users`	utilisateurs authentifiés
`self`	utilisateurs associés à l'objet cible
`dn.regex=<regex>`	Tous les utilisateurs auxquels cette expression rationnelle s'applique

- ⟨*accès*⟩ spécifie le type d'accès. Utilisez les options énumérées dans le tableau 29.3 de la présente page.

TAB. 29.3: *Types d'accès*

Descripteur	Étendue de l'accès
`none`	Accès interdit
`auth`	pour la prise de contact avec le serveur
`compare`	pour l'accès aux objets pour comparaison
`search`	pour l'application de filtres de recherche
`read`	accès en lecture
`write`	accès en écriture

`slapd` compare les privilèges demandés par le client avec ceux qui sont accordés dans le fichier `slapd.conf`. Le client obtient l'accès si les règles permettent des droits plus élevés ou égaux à ceux qui sont demandés. Si le client demande des droits plus élevés que ceux qui sont déclarés dans les règles, l'accès est interdit.

L'exemple 29.5 de la présente page présente un contrôle d'accès simple que vous pouvez configurer à votre guise à l'aide d'expressions rationnelles.

Example 29.5: *slapd.conf: Exemple de contrôle d'accès*

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
   by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
   by user read
   by * none
```

Cette règle stipule que pour tous les enregistrements `ou`, seul l'administrateur concerné dispose de l'accès en écriture. Les autres utilisateurs authentifiés bénéficient d'un accès en lecture et le reste du monde n'a droit à aucun accès.

Astuce

Définition de règles d'accès

En l'absence de règle `access to` ou d'instruction `by` concordante, l'accès n'est pas autorisé. Seuls les droits d'accès spécifiés de manière explicite sont accordés. Dans le cas où aucune règle n'est définie, on applique le principe par défaut : droits en écriture pour l'administrateur et droits en lecture pour le reste du monde.

Astuce

Pour plus d'informations et un exemple de configuration des privilèges d'accès LDAP, reportez-vous à la documentation en ligne du paquetage `openldap2` installé.

Pour la gestion des contrôles d'accès, il est possible d'utiliser, outre le fichier central de configuration du serveur (`slapd.conf`), les ACI, ou informations de contrôle d'accès (de l'anglais Access Control Information). Les ACI permettent d'enregistrer les informations d'accès à différents objets dans l'arborescence LDAP elle-même. Ce mode d'accès étant encore peu diffusé et étant considéré par les développeurs eux-mêmes comme étant de niveau expérimental, nous vous renvoyons ici aux pages correspondantes de la documentation du projet OpenLDAP : `http://www.openldap.org/faq/data/cache/758.html`.

29.3.2 Instructions propres à une base de données dans slapd.conf

Example 29.6: slapd.conf : Instructions propres à une base de données

```
database ldbm
suffix "dc=suse,dc=de"
rootdn "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index   objectClass     eq
```

La première ligne de cette section (voir l'exemple 29.6 de la présente page) définit le type de base de données, en l'occurrence LDBM. Le paramètre `suffix` à la seconde ligne définit la partie de l'arborescence LDAP dont ce serveur doit être responsable. Le `rootdn` suivant indique qui dispose des privilèges d'administrateur sur ce serveur. L'utilisateur indiqué ici ne doit pas pas posséder d'enregistrement LDAP ni exister comme utilisateur normal. L'instruction `rootpw` définit le mot de passe de l'administrateur. Vous pouvez saisir ici à la place de `secret` le hachage du mot de passe de l'administrateur créé avec slappasswd. L'instruction `directory` spécifie le répertoire dans lequel les annuaires de la base de données sont enregistrés sur le serveur. La dernière instruction, `index objectClass eq`, permet de gérer un index à partir des classes d'objets. Le cas échéant, complétez quelques attributs parmi ceux que vous estimez les plus recherchés. Si vous ajoutez vos propres règles `Access` pour la base de données, elles sont utilisées à la place des règles `Access` globales.

29.3.3 Démarrer et arrêter les serveurs

Lorsque vous avez terminé de configurer le serveur LDAP et que vous avez créé tous les enregistrements que vous souhaitiez sur le modèle décrit dans la section 29.4 page ci-contre), démarrez le serveur LDAP en tant qu'utilisateur `root` à l'aide de la commande `rcldap start`. Si vous voulez arrêter le serveur à la

main, saisissez la commande `rcldap stop`. Vous pouvez demander l'état d'exécution du serveur LDAP à l'aide de la commande `rcldapstatus`.

Vous pouvez automatiser le démarrage et l'arrêt du serveur lors de la mise en marche et de l'arrêt de la machine concernée à l'aide de l'éditeur de niveaux d'exécution de YaST décrit dans la section 7.6 page 177. Vous pouvez aussi créer vous-même les liens correspondants pour les scripts de démarrage et d'arrêt à l'aide de la commande `insserv` à partir d'une invite de commande comme décrit dans la section 7.5.1 page 175).

29.4 Manipulation de données dans l'annuaire LDAP

OpenLDAP met à votre disposition toute une série de programmes pour la gestion des données dans l'annuaire LDAP. Nous présenterons ci-après les quatre principaux d'entre eux pour les opérations d'ajout, de suppression, de recherche et de modification de données.

29.4.1 Créer des données dans l'annuaire LDAP

Une fois que la configuration de votre serveur LDAP dans `/etc/openldap/slapd.conf` est correcte et opérationnelle (c'est-à-dire qu'elle comporte les indications appropriées pour `suffix`, `directory`, `rootdn`, `rootpw` et `index`), vous pouvez commencer à ajouter des enregistrements. OpenLDAP propose à cet effet le programme `ldapadd`. Pour des raisons pratiques, il est recommandé, dans la mesure du possible, d'ajouter les objets à la base de données par groupes. LDAP sait interpréter le format LDIF (de l'anglais LDAP Data Interchange Format, format d'échange de données LDAP). Un fichier LDIF est un fichier texte simple comportant un nombre quelconque de paires attribut-valeur. Les classes d'objets et les attributs disponibles figurent dans les fichiers schémas spécifiés dans `slapd.conf`. Le fichier LDIF destiné à créer un schéma grossier pour l'exemple dans la figure 29.1 page 521 se présenterait comme dans l'exemple 29.7 page suivante).

Example 29.7: Exemple de fichier LDIF

```
# L'organisation SUSE
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SUSE AG
dc: suse

# L'unité d'organisation Développement (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# L'unité d'organisation Documentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# L'unité d'organisation Informatique interne (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

Important

Codage des fichiers LDIF

LDAP utilise le codage UTF-8 (Unicode). Par conséquent, les caractères accentués doivent être convenablement codés à la saisie. Utilisez un éditeur qui prend en charge UTF-8 (comme Kate ou les versions récentes d'Emacs). Sinon, évitez les lettres accentués et autres caractères spéciaux ou utilisez `recode` pour ré-encoder les données saisies en UTF-8.

Important

Enregistrez le fichier sous le nom `<fichier>.ldif` et transférez-le sur le serveur à l'aide de la commande suivante :

```
ldapadd -x -D <dn de l'administrateur> -W -f <fichier>.ldif
```

L'option `-x` désactive dans ce cas à l'authentification via SASL. L'option `-D` désigne l'utilisateur chargé de cette opération ; saisissez ici le DN valide de l'administrateur tel qu'il a été configuré dans `slapd.conf`. Dans notre exemple, nous aurions `cn=admin,dc=suse,dc=de`. L'option `-W` permet d'éviter de saisir le mot de passe sur la ligne de commande (en clair) et active une demande de mot de passe séparée. Le mot de passe en question a été créé précédemment dans `slapd.conf` avec l'option `rootpw`. Le paramètre `-f` indique le nom du fichier. Vous pouvez voir dans l'exemple 29.8 de la présente page le détail de l'appel de `ldapadd`.

Example 29.8: *ldapadd de exemple.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f exemple.ldif

Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

Vous pouvez spécifier les données liées aux utilisateurs dans des fichiers LDIF séparés. L'exemple 29.9 de la présente page ajoute l'utilisateur `Tux` au nouvel annuaire LDAP.

Example 29.9: *Fichier LDIF pour Tux*

```
# Employé Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@suse.de
uid: tux
telephoneNumber: +33 12 34 56 78 90
```

Un fichier LDIF peut comporter un nombre quelconque d'objets. Vous pouvez transférer au serveur des arborescences complètes ou uniquement des parties telles que des objets distincts. Si vous devez modifier vos données selon une fréquence relativement élevée, il est recommandé de définir une granularité fine avec des objets distincts, ce qui permet de faciliter le travail de recherche de l'objet à modifier dans un fichier de grande taille.

29.4.2 Modifier des données dans l'annuaire LDAP

Lorsque vous voulez modifier des données, utilisez le programme `ldapmodify`. Le plus simple consiste à modifier dans un premier temps le fichier LDIF concerné, puis à passer le fichier modifié au serveur LDAP. Ainsi, pour changer le numéro de téléphone de l'employé `Tux` de `+33 12 34 56 78 90` en `+33 12 34 56 78 45`, éditez le fichier LDIF, comme indiqué dans l'exemple 29.10 de la présente page.

Example 29.10: *Fichier LDIF modifié tux.ldif*

```
# Employé Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +33 12 34 56 78 45
```

Importez le fichier modifié dans l'annuaire LDAP à l'aide de la commande suivante :

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

Autre possibilité : utiliser `ldapmodify` pour spécifier directement sur la ligne de commande les attributs à modifier. La procédure est la suivante :

1. Exécutez la commande `ldapmodify` et saisissez votre mot de passe :

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W

   Enter LDAP password:
   ```

2. Faites vos modifications dans l'ordre suivant, en respectant la syntaxe indiquée ci-après :

   ```
   dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
   changetype: modify
   replace: telephoneNumber
   telephoneNumber: +33 12 34 56 78 45
   ```

Pour plus d'informations sur la commande `ldapmodify` et sur sa syntaxe, reportez-vous à la page de manuel correspondante (ldapmodify(1)).

29.4.3 Chercher ou extraire les données d'un annuaire LDAP

OpenLDAP fournit avec le programme `ldapsearch` un utilitaire en ligne de commande pour chercher des données dans un annuaire LDAP et pour en extraire des données. Une commande simple de recherche utiliserait la syntaxe suivante :

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

L'option `-b` définit la base de la recherche, c'est-à-dire la partie de l'arbre dans laquelle la recherche doit se faire. Il s'agit dans le cas présent de `dc=suse, dc=de`. Pour effectuer une recherche plus fine dans des sous-domaines donnés de l'annuaire LDAP (par exemple uniquement dans la division `devel`), utilisez `-b` pour passer cette branche. `-x` indique qu'il faut utiliser une authentification simple. `(objectClass=*)` vous permet de décider que vous voulez lire tous les objets contenus dans votre annuaire. Utilisez cette commande après avoir constitué une nouvelle arborescence afin de vérifier si tous vos enregistrements ont été convenablement mis en place et si le serveur répond comme convenu. Vous trouverez des informations supplémentaires sur l'utilisation du programme `ldapsearch` dans la page de manuel correspondante (ldapsearch(1)).

29.4.4 Supprimer des données d'un annuaire LDAP

Supprimez les enregistrements dont vous n'avez plus besoin à l'aide du programme `ldapdelete`. La syntaxe est analogue à celle des commandes précédemment décrites. Ainsi, pour supprimer complètement du système l'enregistrement de l'utilisateur `Tux Linux`, vous devez saisir la commande suivante :

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

29.5 Le client LDAP de YaST

YaST fournit un module pour administrer des utilisateurs avec LDAP. Si vous n'avez pas activé cette fonctionnalité lors de l'installation, démarrez le module en choisissant 'Services réseau' → 'Client LDAP'. YaST effectue automatiquement les modifications de PAM et NSS requises pour LDAP (voir ci-dessous) et installe les fichiers nécessaires.

29.5.1 Procédure normale

Pour comprendre le fonctionnement du module client LDAP de YaST, vous devez connaître les processus s'exécutant en arrière-plan sur votre machine cliente. Si vous activez LDAP pour l'authentification réseau pendant l'installation ou si vous appelez le module de YaST, les paquetages `pam_ldap` et `nss_ldap` sont installés et les deux fichiers de configuration correspondants sont modifiés. `pam_ldap` est le module PAM responsable de la communication entre les processus de connexion et l'annuaire LDAP utilisé comme source des données d'authentification. Le module dédié `pam_ldap.so` est installé et la configuration de PAM est modifiée (voir l'exemple 29.11 de la présente page).

Example 29.11: *pam_unix2.conf modifié pour LDAP*

```
auth:       use_ldap nullok account:    use_ldap password:
     use_ldap nullok session:    none
```

Si vous souhaitez configurer à la main des services supplémentaires pour les utiliser avec LDAP, ajoutez le module LDAP PAM au fichier de configuration de PAM dans `/etc/pam.d/`. Vous trouverez des fichiers de configuration déjà adaptés à différents services dans `/usr/share/doc/packages/pam_ldap/pam.d/`. Copiez les fichiers correspondants dans `/etc/pam.d/`.

Modifiez la résolution de noms de la bibliothèque `glibc` à l'aide du programme `nss_ldap` en utilisant le mécanisme `nsswitch` pour permettre l'utilisation de LDAP. En installant ce paquetage, un nouveau fichier `nsswitch.conf` modifié est enregistré dans `/etc`. Pour plus de précisions sur le fonctionnement de `nsswitch.conf`, reportez-vous à la section 22.5.1 page 448. Pour la gestion des utilisateurs ou leur authentification avec LDAP, votre fichier `nsswitch.conf` doit comporter les lignes suivantes. Voir l'exemple 29.12 de la présente page.

Example 29.12: *Adaptations dans nsswitch.conf*

```
passwd: compat group: compat passwd_compat: ldap group_compat: ldap
```

Ces lignes demandent à la bibliothèque de résolution de `glibc` d'évaluer dans un premier temps les fichiers correspondants dans le répertoire `/etc` et d'accéder ensuite au serveur LDAP. Vous pouvez tester ce mécanisme par exemple en

lisant le contenu de la base de données d'utilisateurs à l'aide de de la commande `getent passwd`. Le résultat doit présenter aussi bien les utilisateurs locaux présents sur votre système que tous les utilisateurs présents sur le serveur LDAP.

Si vous voulez empêcher que les utilisateurs normaux administrés par LDAP ne puissent se connecter au serveur à l'aide de `ssh` ou de `login`, vous devez ajouter une ligne dans `/etc/passwd` et `/etc/group` : `+::::::/sbin/nologin` dans `/etc/passwd` et `+:::` dans `/etc/group`.

29.5.2 Configuration du client LDAP

Une fois que `nss_ldap`, `pam_ldap`, `/etc/passwd` et `/etc/group`ont été convenablement modifiés par YaST, vous pouvez commencer les opérations de configuration à proprement parler dans la première boîte de dialogue de YaST. Reportez-vous à la figure 29.2 de la présente page.

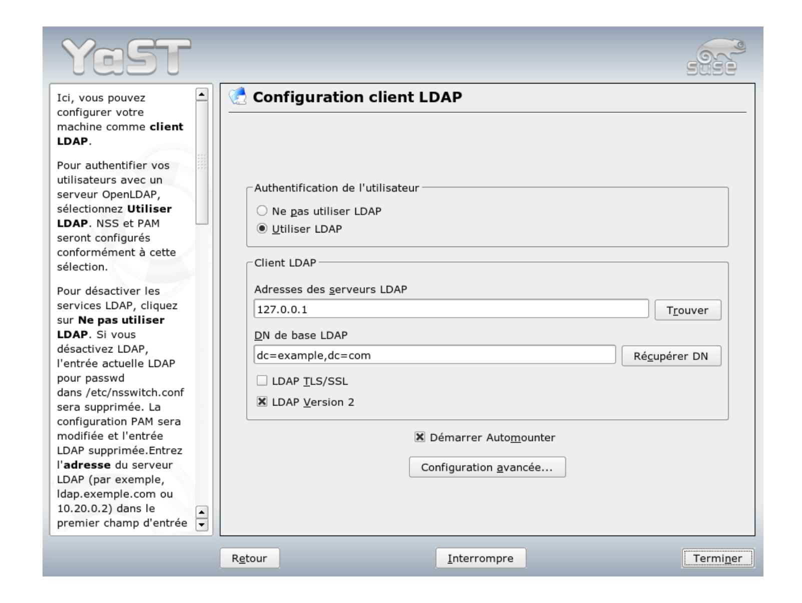


FIG. 29.2: *YaST~: Configuration du client LDAP*

Activez l'utilisation de LDAP pour l'authentification des utilisateurs dans la première boîte de dialogue. Saisissez la base de recherche dans laquelle toutes les

données sont enregistrées dans le serveur LDAP dans 'DN de base LDAP'. Saisissez l'adresse du serveur LDAP dans 'Adresses des serveurs LDAP'. Pour monter automatiquement des répertoires sur des hôtes distants, choisissez 'Démarrer Automounter'. Pour éditer des données sur le serveur en tant qu'administrateur, cliquez sur 'Configuration avancée'. Reportez-vous à la figure 29.3 de la présente page.

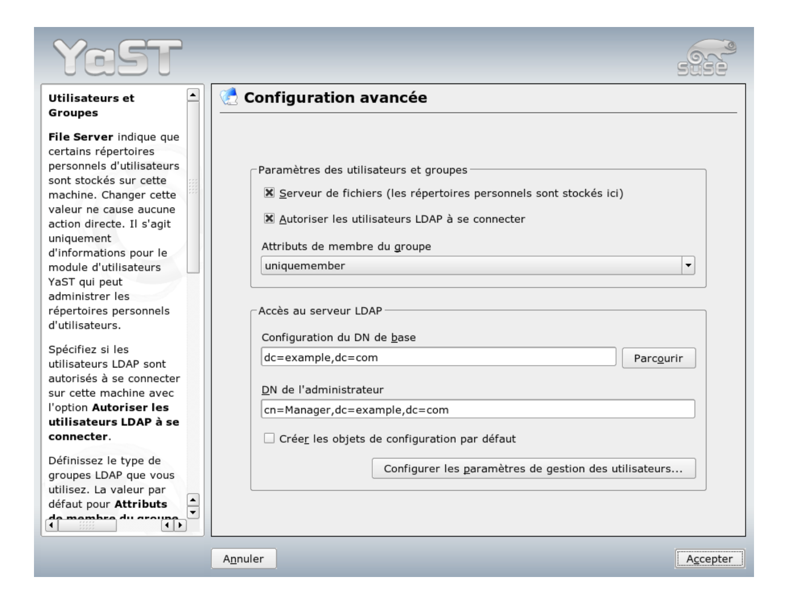


FIG. 29.3: *YaST~: Configuration avancée*

La page suivante est divisé en deux : dans la partie supérieure, procédez à la configuration des paramètres généraux pour utilisateurs et groupes qui déterminent le comportement du module utilisateurs de YaST. Dans la partie inférieure, saisissez les données d'accès au serveur LDAP. Les paramètres relatifs aux utilisateurs et groupes se limitent aux entrées suivantes :

Serveur de fichiers Ce système est-il un serveur de fichiers et administre les répertoires `/home` des utilisateurs ? En activant la case à cocher, vous indiquez au module utilisateurs de YaST comment agir avec les répertoires personnels des utilisateurs sur ce système.

Autoriser la connexion des utilisateurs LDAP
Activez la case à cocher afin d'autoriser la connexion au système des utilisateurs administrés par LDAP.

Attribut pour membres du groupe Définissez le type de groupe LDAP à utiliser. Vous avez le choix entre : 'member' (configuration par défaut) et 'uniquemember'.

Pour modifier des configurations sur le serveur LDAP, saisissez dans cette boîte de dialogue les données d'accès requises (voir la figure 29.3 page précédente). Il s'agit de la zone d'édition 'Configuration du DN de base' (dans laquelle tous les objets de configuration sont enregistrés) et de la zone d'édition 'DN d'administrateur'.

Pour éditer les enregistrements sur le serveur LDAP, cliquez sur le bouton 'Configurer les paramètres de gestion des utilisateurs'. Une boîte de dialogue apparaît, dans laquelle vous êtes invité à saisir votre mot de passe LDAP pour vous authentifier sur le serveur. Les ACL ou ACI sur le serveur vous permettent ensuite d'accéder aux modules de configuration sur le serveur.

Important

Mise en œuvre du client de YaST

Le client LDAP de YaST est utilisé pour ajuster, et le cas échéant agrandir, de manière appropriée les modules de YaST, en fonction de la gestion des utilisateurs et des groupes. Parallèlement à cela, vous avez la possibilité de définir des formulaires avec des valeurs par défaut pour les différents attributs, de manière à simplifier la saisie à proprement parler des données. Les valeurs par défaut créées ici sont elles-mêmes enregistrées dans l'annuaire LDAP sous forme d'objets LDAP. La saisie des données utilisateurs continue à être réalisé à l'aide des formulaires de modules de YaST normaux. Les informations saisies sont enregistrées sous forme d'objets dans l'annuaire LDAP.

Important

La boîte de dialogue de configuration du module (figure 29.4 page suivante, vous permet de choisir et de modifier des modules de configuration existants, d'en créer de nouveaux ou de créer et modifier des modèles (en anglais templates) pour ces modules. Pour modifier une valeur dans un module de configuration ou pour renommer un module, choisissez le type de module au-dessus du sommaire du module courant. Une liste sous forme de table apparaît alors dans la vue de détail avec l'ensemble des attributs et des valeurs associées autorisés dans ce module. En plus des attributs définis, la liste contient aussi tous les autres attributs autorisés par le schéma utilisé mais qui ne sont pas utilisés actuellement.

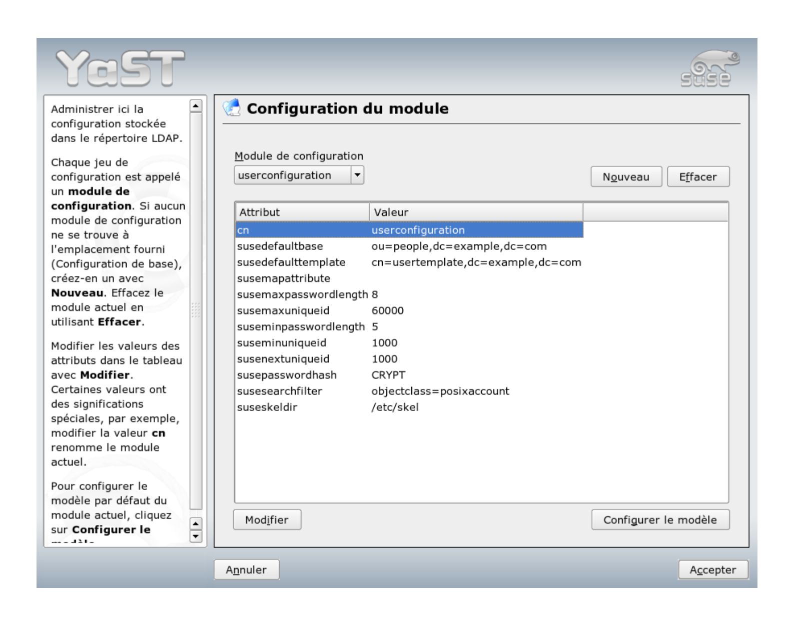


FIG. 29.4: *YaST~: configuration du module*

Si vous voulez copier un module, il suffit de modifier `cn`. Pour modifier individuellement des valeurs d'attributs, choisissez-les dans la liste de contenu et cliquez sur le bouton 'Modifier'. Une boîte de dialogue s'ouvre alors à partir de laquelle vous pouvez modifier tous les paramètres de l'attribut. Validez vos modifications en cliquant sur le bouton 'OK'.

Si vous souhaitez compléter les modules existants par l'ajout d'un nouveau module, cliquez sur le bouton 'Nouveau' au-dessus du sommaire. Saisissez dans la boîte de dialogue qui s'ouvre alors le nom et la classe d'objet du nouveau module (soit `suseuserconfiguration` soit `susegroupconfiguration`). Lorsque vous sortez de cette boîte de dialogue en cliquant sur le bouton 'OK', le nouveau module est ajouté à la liste de sélection des modules présents et peut être sélectionné ou désélectionné à l'aide de la liste déroulante. Pour supprimer le module choisi, cliquez sur le bouton 'Supprimer'.

Les modules de YaST pour la gestion des utilisateurs et des groupes intègrent des modèles utilisant des valeurs par défaut appropriées si vous les avez précédemment définies à l'aide des clients LDAP de YaST. Pour éditer un modèle à votre convenance, cliquez sur le bouton 'Configurer le modèle'. Le menu déroulant

affiche des modèles existants modifiables ou un enregistrement vide. Choisissez l'un de ces modèles et configurez dans le formulaire suivant 'Configuration modèle de l'objet' les propriétés de ce modèle (voir la figure 29.5 de la présente page). Ce formulaire est composé de deux volets sous forme de table. Le volet supérieur comporte tous les attributs généraux du modèle. Définissez leurs valeurs conformément à vos besoins ou laissez-les vides. Les attributs vides sont supprimés du serveur LDAP.

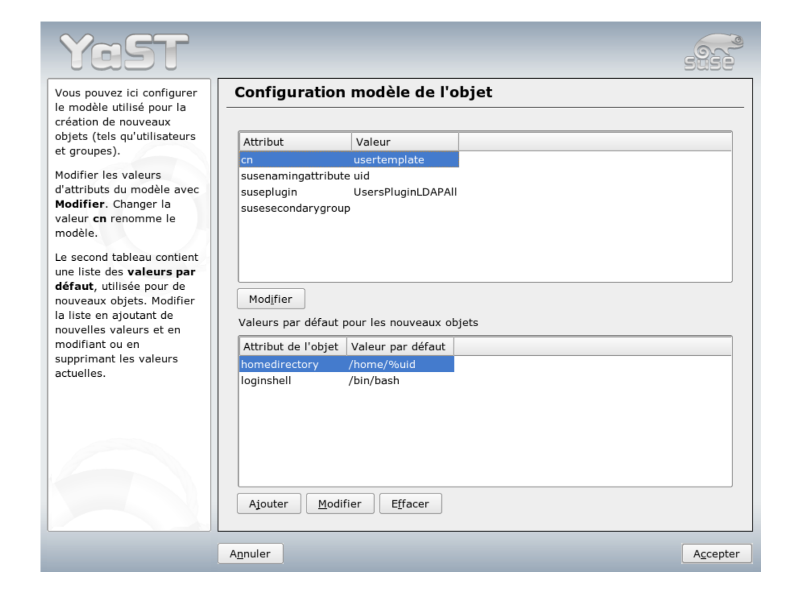


FIG. 29.5: *YaST~: Configuration d'un modèle d'objet*

La deuxième liste ('Valeurs par défaut pour les nouveaux objets') énumère tous les attributs de l'objet LDAP correspondant (ici : la configuration des groupes ou des utilisateurs), pour lesquels vous définissez une valeur par défaut. Vous pouvez ajouter d'autres attributs et leurs valeurs par défaut ainsi que supprimer des attributs. Un modèle peut être simplement copié, à la manière d'un module, en modifiant l'enregistrement `cn`, afin de créer un nouveau modèle. Reliez le modèle au module associé en fixant la valeur d'attribut de `susedefaulttemplate` du module au DN du modèle modifié, conformément à la procédure indiquée précédemment.

Astuce

Vous pouvez créer des valeurs par défaut pour un attribut formé à partir d'autres attributs, en utilisant une syntaxe avec des variables plutôt qu'une valeur absolue. Ainsi, `cn=%sn %givenName` est automatiquement créé lors de la création d'utilisateur à partir des valeurs d'attribut de `sn` et de `givenName`.

Astuce

Lorsque tous les modules et modèles sont convenablement configurés et qu'ils sont opérationnels, créez à l'aide de YaST de nouveaux groupes et utilisateurs, en suivant la procédure habituelle.

29.5.3 Utilisateurs et groupes—Configuration avec YaST

Après avoir configuré des modules et des modèles pour le réseau, la saisie des données relatives aux utilisateurs et aux groupes diffère très légèrement de la procédure n'utilisant pas LDAP. Les instructions sommaires suivantes concernent la gestion des utilisateurs, la procédure appliquée à la gestion des groupes étant analogue.

Vous pouvez accéder à la gestion des utilisateurs de YaST grâce à 'Sécurité et Utilisateurs' → 'Modifier et créer des utilisateurs'. Pour ajouter un nouvel utilisateur, cliquez sur le bouton 'Ajouter'. Un formulaire s'ouvre alors pour saisir des principales données utilisateurs comme le nom, l'identifiant de connexion et le mot de passe. Le bouton 'Détails' vous permet d'accéder à un formulaire pour configurer configurer l'appartenance à d'autres groupes, l'interpréteur de commande utilisé à la connexion et le répertoire personnel. Les valeurs par défaut des zones de saisie ont été définies selon la procédure décrite dans la section 29.5.2 page 535. Si vous utilisez LDAP, ce formulaire mène à un autre formulaire de saisie des attributs LDAP. Ce formulaire est illustré dans la figure 29.6 page suivante) . Choisissez tous les attributs dont vous souhaitez modifier la valeur et cliquez sur le bouton 'Modifier' pour ouvrir la fenêtre d'édition correspondante. Sortez ensuite de ce formulaire en cliquant sur le bouton 'Suivant', ce qui vous fait revenir au formulaire initial de la gestion des utilisateurs.

Vous pouvez accéder à des 'Options LDAP' à partir du formulaire initial de gestion des utilisateurs. Ceci vous permet d'appliquer des filtres de recherche LDAP à l'ensemble des utilisateurs disponibles ou d'entrer dans le module de configuration des utilisateurs et groupes LDAP en choisissant 'Configuration des utilisateurs et groupes LDAP'.

FIG. 29.6: *YaST~: Paramètres LDAP supplémentaires*

29.6 Informations supplémentaires

Nous avons volontairement renoncé à traiter dans ce chapitre des sujets plus complexes tels que la configuration SASL ou la mise en place d'un serveur LDAP répliqué qui se partage la tâche avec plusieurs "esclaves". Pour plus d'informations sur ces deux sujets, reportez-vous au document *OpenLDAP 2.2 Administrator's Guide* (voir lien ci-après).

Vous trouverez sur le site web du projet OpenLDAP une documentation complète pour les utilisateurs de LDAP débutants et avancés :

OpenLDAP Faq-O-Matic Un recueil très riche de questions et de réponses sur l'installation, la configuration et l'utilisation de OpenLDAP. `http://www.openldap.org/faq/data/cache/1.html` (en anglais).

Quick Start Guide [Guide de démarrage rapide]
Un guide concis pour votre premier serveur LDAP.
`http://www.openldap.org/doc/admin22/quickstart.html` ou

dans le système installé à l'emplacement /usr/share/doc/packages/openldap2/admin-guide/quickstart.html.

OpenLDAP 2.2 Administrator's Guide [Guide de l'administrateur OpenLDAP 2.2]

Une introduction complète à tous les domaines importants de la configuration LDAP,y compris le contrôle d'accès et le chiffrement : http://www.openldap.org/doc/admin22/ ou dans le système installé à l'emplacement /usr/share/doc/packages/openldap2/admin-guide/index.html

Par ailleurs les livres rouges d'IBM indiqués ci-après se penchent sur LDAP :

Understanding LDAP [Comprendre LDAP]

Une introduction générale et très complète aux principes de base de LDAP : http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf

LDAP Implementation Cookbook [Recettes pour la mise en pratique de LDAP]

L'audience cible de ce document correspond aux administrateurs de *IBM SecureWay Directory*. On trouve toutefois également d'importantes informations d'ordre général sur LDAP dans : http://www.redbooks.ibm.com/redbooks/pdfs/sg245110.pdf

Documents imprimés en anglais sur LDAP :

- Howes, Smith & Good: *Understanding and Deploying LDAP Directory Services*. Addison-Wesley, 2ème éd., 2003. - (ISBN 0-672-32316-8)
- Hodges: *LDAP System Administration*. O'Reilly & Associates, 2003. - (ISBN 1-56592-491-6)

Les RFC (Request for comments) 2251 à 2256 sont des documents de référence faisant autorité sur LDAP.

Le serveur web Apache

Avec une part de marché de plus de soixante pour cent, Apache est le serveur web le plus répandu dans le monde (source : `http://www.netcraft.com`). Pour des applications web, Apache est souvent combiné avec Linux, la base de données MySQL et les langages de programmation PHP et Perl. Cette combinaison est habituellement désignée par l'abréviation *LAMP*.

Nous présentons dans ce chapitre le serveur web Apache. Nous vous expliquons ici comment l'installer et le configurer et nous décrivons également quelques-uns des modules disponibles. Les variantes pour les hôtes virtuels sont également abordées.

30.1 Notions de base

Cette section traite des principes fondamentaux des serveurs web et des protocoles qu'ils utilisent. Les fonctionnalités les plus importantes sont également introduites.

30.1.1 Serveur web

Un serveur web fournit à un client les pages HTML qu'il demande. Ces pages peuvent être stockées dans un répertoire (pages passives ou statiques) ou générées comme réponse à une requête (contenus actifs).

30.1.2 HTTP

Les clients sont dans la plupart des cas des navigateurs web comme Konqueror ou Mozilla. La communication entre le navigateur et le serveur web se fait par le protocole HTTP (Hypertext Transfer Protocol). La version actuelle, HTTP 1.1; est documentée dans le RFC 2068 ainsi que dans sa mise à jour RFC 2616. Ces RFC se trouvant à l'adresse `http://www.w3.org`.

30.1.3 URL

Les clients demandent des pages au serveur par le biais d'un URL comme `http://www.novell.com/linux/suse/`. Un URL est composé des éléments suivants :

Protocole Les protocoles souvent utilisés sont :

- **http://** Le protocole HTTP
- **https://** Version sécurisée et chiffrée de HTTP
- **ftp://** File Transfer Protocol (Protocole de Transfert de Fichiers), pour le téléchargement de fichiers.

Domaine Dans notre exemple, `www.novell.com`. Le domaine peut encore être subdivisé, la première partie `www` faisant référence à un ordinateur et la deuxième partie `novell.com` au domaine proprement dit. Ces deux parties considérées ensemble sont également appelées FQDN (Fully Qualified Domain Name, nom de domaine pleinement qualifié).

Ressource Dans notre cas, `index.html`. Cette partie indique le chemin d'accès complet à cette ressource. Cette ressource peut être un fichier, comme dans notre cas. Il peut également s'agir d'un script CGI, d'une page de serveur Java ou tout autre type de ressource.

Ici, les mécanismes d'Internet responsables de l'acheminement d'une requête, comme le Domain Name System – Système de Noms de Domaines ou DNS, transmettent la requête au domaine `www.suse.fr` et la redirigent vers le ou les ordinateurs hébergeant les ressources. Apache fournit alors la ressource, dans notre exemple la page `index.html`, depuis son répertoire de fichiers. Dans ce cas, le fichier se trouve dans le répertoire de niveau le plus élevé ; il peut cependant aussi se trouver dans un sous-répertoire, comme dans `http://support.novell.com/linux/`.

Ici, le chemin d'accès du fichier est relatif à la racine des documents (`DocumentRoot`), qui peut être modifiée dans le fichier de configuration. La section DocumentRoot page 551 décrit les modifications à effectuer.

30.1.4 Affichage automatique d'une page par défaut

Dans le cas ou aucune page par défaut n'est précisée, Apache ajoute automatiquement à l'URL l'un des noms les plus courants pour ces pages. Le nom le plus fréquent pour ces pages est `index.html`. La section DirectoryIndex page 552 décrit comment configurer cette fonctionnalité d'Apache et quels noms de page il doit utiliser. Dans notre exemple, il suffit d'appeler `http://www.suse.com` pour que le serveur renvoie la page `http://www.novell.com/linux/suse/`.

30.2 Installation du serveur HTTP avec YaST

Vous pouvez installer Apache facilement avec YaST, mais vous devrez disposer de quelques connaissances sur le sujet si vous avez l'intention de mettre en place un serveur web de cette manière. Après avoir choisi 'Services réseau' → 'Serveur HTTP' dans le centre de contrôle de YaST, il vous sera peut-être demandé de confirmer l'installation de certains paquetages manquants. Dès que tout est installé, YaST affiche la boite de dialogue de configuration ('Configuration du serveur HTTP').

Activez-y tout d'abord le 'Service HTTP'. Le port correspondant du pare-feu (port 80) est alors également ouvert ('Ouvrir le pare-feu sur les ports sélectionnés'). Dans la partie inférieure de la fenêtre ('Paramètres/Résumé') on peut configurer le serveur HTTP local : 'Listen on' (l'option par défaut est `Port 80`), 'Modules', 'Hôte par défaut' et 'Hôtes'. 'Modifier' permet de changer les paramètres actuels.

Vérifiez d'abord l''Hôte par défaut' et adaptez le cas échéant la configuration à vos besoins. Activez ensuite dans 'Modules' les modules désirés. Les boites de dialogue suivantes vous permettent de configurer en détail le serveur, en particulier de régler les paramètres des hôtes virtuels.

30.3 Les modules d'Apache

On peut ajouter de nombreuses fonctions à Apache par le biais de modules. Par exemple, Apache peut exécuter des scripts CGI dans différents langages de programmation en utilisant de tels modules. En plus de Perl et PHP, d'autres langages de scripts sont à votre disposition comme Python ou Ruby. Il existe aussi des modules pour le transfert sécurisé de données via SSL (Secure Sockets Layer - Couche de connexion sécurisée), pour l'authentification des utilisateurs, pour la journalisation avancée et bien plus encore.

Avec des connaissances suffisantes, il est possible de développer des modules pour Apache afin de l'adapter suivant vos besoins et vos préférences. Pour de plus amples informations sur ce sujet, veuillez vous référer à la section 30.12.4 page 567.

Vous pouvez indiquer différents gestionnaires ("handlers") pour traiter les requêtes au moyen de directives contenues dans le fichier de configuration. Ces gestionnaires peuvent soit être partie intégrante d'Apache, soit être utilisés sous la forme de modules appelés pour traiter la requête, ce qui confère une grande flexibilité à cette procédure. Il est aussi possible d'utiliser vos propres modules avec Apache et ainsi influencer la façon dont les requêtes sont traitées.

Avec Apache, la modularité va très loin car, à l'exception de quelques tâches mineures, tout est géré par des modules. La progression a été telle que même HTTP est géré par le biais de modules. En conséquence, Apache n'est pas forcément un serveur web. Il peut aussi assurer des tâches totalement différentes grâce à d'autres modules. Par exemple, un serveur de messagerie POP3 basé sur Apache existe au titre d'étude de faisabilité.

Les modules Apache offrent plusieurs possibilités complémentaires très utiles :

Hôtes virtuels La prise en charge des hôtes virtuels permet d'exploiter plusieurs sites web avec une seule instance d'Apache fonctionnant sur une unique machine physique. Pour l'utilisateur final, le serveur apparaît comme plusieurs serveurs indépendants. Les hôtes virtuels peuvent être configurés sur des adresses IP différentes ou sur la base des noms de domaine. Cela permet d'économiser les coûts d'acquisition et la charge de travail d'administration qui serait nécessaire pour plusieurs ordinateurs supplémentaires.

Transcription flexible d'URL Apache offre une multitude de possibilités de manipulation et de transcription d'URL (URL rewriting). Pour de plus amples informations, consultez la documentation d'Apache.

Négociation de contenu Apache peut fournir au client (navigateur) une page adaptée à ses capacités. Par exemple, des versions simples et sans cadres d'une page donnée peuvent être transmises aux navigateurs anciens ou ne fonctionnant qu'en mode texte, comme Lynx. De manière similaire, on peut éviter l'incompatibilité de certains navigateurs avec JavaScript en fournissant aux différents navigateurs une version adaptée des pages web. Cela implique bien sûr d'adapter le code JavaScript à chaque navigateur.

Gestion d'erreurs flexible En cas d'erreur (par exemple lorsqu'une page n'est pas disponible), il est possible de réagir de façon flexible et de donner une réponse appropriée. Cette réponse peut même être générée dynamiquement, par exemple à l'aide d'un script CGI.

30.4 Les fils d'exécution (threads)

Un fil d'exécution (thread) est une sorte de processus "léger". L'avantage d'un fil d'exécution, comparé à un vrai processus, est qu'il consomme beaucoup moins de ressources. Par conséquent, utiliser des fils d'exécution à la place de processus améliore les performances. L'inconvénient est que les applications exécutées dans un environnement à base de fils d'exécution doivent être thread-safe. Cela signifie que :

- Les fonctions (ou dans le cas d'applications orientées objet, les méthodes) doivent être "réentrantes"—une fonction avec les mêmes données en entrée fournit toujours le même résultat, même si d'autres fils d'exécution utilisent simultanément cette même fonction. En conséquence, les fonctions doivent être programmées de façon à pouvoir être appelées par plusieurs fils d'exécution en même temps.

- L’accès aux ressources (en général des variables) doit être configuré de manière à éviter les conflits entre les fils d’exécution qui se déroulent en même temps.

Apache 2 gère les requêtes soit en tant que processus séparés, soit dans un mode mixte qui combine des processus et des fils d’exécution. L’exécution en tant que processus est réalisée par le MPM "prefork". L’exécution en tant que fil d’exécution est réalisée par le MPM "worker". Le choix du MPM à utiliser s’effectue lors de l’installation (voir la section 30.5 de la présente page).Le troisième mode— *perchild*— n’a pas encore acquis une maturité suffisante, il n’est donc pas (encore) disponible dans SUSE LINUX.

30.5 Installation

30.5.1 Choix des paquetages dans YaST

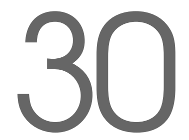
Pour une installation de base, il suffit de choisir le paquetage Apache `apache2`. Vous devez de plus installer un des paquetages MPM (Multiprocessing Module —Module de Multitraitement) tel que `apache2-prefork` ou `apache2-worker`. Lorsque vous choisissez un MPM, gardez à l’esprit le fait que le MPM "Worker", qui fonctionne par fils d’exécution, ne peut pas être utilisé conjointement avec `mod_php4` car les bibliothèques de `mod_php4` ne sont pas encore thread-safe.

30.5.2 Activation d’Apache

Une fois installé, il faut activer Apache comme service dans l’éditeur de niveaux d’exécution. Pour démarrer Apache à l’amorçage du système, cochez dans l’éditeur de niveau d’exécution les niveaux 3 et 5. Pour vérifiersi Apache fonctionne, demandez l’URL `http://localhost` dans un navigateur. Si Apache fonctionne, on peut alors voir une page d’exemple si le paquetage `apache2-example-pages` est installé.

30.5.3 Les modules pour les contenus dynamiques

Pour utiliser des contenus dynamiques à l’aide de modules, installez en plus les modules pour les différents langages de programmation. Il s’agit du paquetage `apache2-mod_perl` pour Perl, du paquetage `mod_php4` pour PHP et enfin du paquetage `mod_python` pour Python. L’utilisation de ces modules est décrite dans la section 30.8.4 page 558.



30.5.4 Paquetages supplémentaires recommandés

Il est en outre recommandé d'installer la documentation fournie dans le paquetage `apache2-doc`. Après l'installation de ce paquetage et l'activation du serveur comme décrit en la section 30.5.2 page précédente), on peut accéder à la documentation directement avec l'URL `http://localhost/manual`.

Si vous voulez développer des modules pour Apache ou compiler des modules provenant d'autres fournisseurs, vous devez aussi installer le paquetage `apache2-devel`, ainsi que les outils de développement correspondants. Ceux-ci contiennent, entre autres, les outils `apxs`, décrits plus en détail dans la section 30.5.5 de la présente page.

30.5.5 Installation de modules avec apxs

`apxs2` est un outil important pour les développeurs de modules. Ce programme permet de compiler et d'installer en une seule commande des modules à partir du code source, tout en effectuant les modifications nécessaires dans lesfichiers de configuration. De plus, il est également possible d'installer des modules se présentant sous forme de fichiers objet (d'extension `.o`) ou comme des bibliothèques statiques (d'extension `.a`). `apxs2` génère à partir de ces sources un objet partagé dynamique (Dynamic Shared Object—DSO) qui peut être utilisé directement comme module par Apache.

L'installation d'un module à partir du code source s'effectue avec la commande `apxs2 -c -i -a mod_chose.c`. D'autres options d'`apxs2` sont décrites dans la page de manuel s'y rapportant. Les modules doivent être activés dans la section `APACHE_MODULES` du fichier `/etc/sysconfig/apache2`, comme décrit dans la section 30.6.1 page suivante.

Il existe plusieurs versions d'`apxs2` : `apxs2`, `apxs2-prefork` et `apxs2-worker`. Tandis qu'`apxs2` installe un module de telle manière qu'il peut être utilisé par les deux MPM, les deux autres programmes installent les modules de telle sorte qu'ils ne seront utilisés que par leur MPM respectif (donc prefork ou worker). `apxs2` installe les modules dans `/usr/lib/apache2`, tandis que `apxs2-prefork` installe les modules dans `/usr/lib/apache2-prefork`.

30.6 Configuration

Une fois Apache installé, les modifications ne sont nécessaires que si vous avez des besoins ou souhaits particuliers. Vous pouvez configurer Apache via YaST ou SuSEconfig ou en éditant directement le fichier `/etc/apache2/httpd.conf`.

30.6.1 Configuration avec SuSEconfig

SuSEconfig reporte les réglages effectués dans `/etc/sysconfig/apache2` dans les d'Apache. Les options de configuration qui y sont proposées devraient être suffisantes pour la plupart des cas. Le fichier contient des commentaires expliquant les effets de chaque variable.

Fichiers de configuration personnalisés

Au lieu de modifier la configuration directement dans le fichier `/etc/apache2/httpd.conf`, vous pouvez, à l'aide de la variable `APACHE_CONF_INCLUDE_FILES`, indiquer votre propre fichier de configuration (tel que `httpd.conf.local`). Celui-ci sera interprété par le fichier de configuration principal. De cette manière, les changements de configuration sont conservés même si le fichier `/etc/apache2/httpd.conf` est écrasé lors d'une réinstallation.

Les modules

Vous pouvez activer les modules installés grâce à YaST en ajoutant le nom du module dans liste indiquée pour la variable `APACHE_MODULES`. Vous trouverez cette variable dans le fichier `/etc/sysconfig/apache2`.

Les drapeaux (flags)

La variable `APACHE_SERVER_FLAGS` permet d'indiquer des drapeaux (flags) qui activent et désactivent certaines sections dans le fichier de configuration. Si une section dans le fichier de configuration est incluse dans les lignes suivantes :

```
<IfDefine un_drapeau> . . . </IfDefine>
```

celle-ci ne sera activée que si le drapeau correspondant est positionné dans la variable `ACTIVE_SERVER_FLAGS` : `ACTIVE_SERVER_FLAGS= un_drapeau` On peut ainsi activer ou désactiver simplement de vastes sections du fichier de configuration en guise de test.

30.6.2 Configuration manuelle

Pour activer des modifications qui ne sont pas possibles au moyen des paramètres de `/etc/sysconfig/apache2`, éditez le fichier de configuration `/etc/apache2/httpd.conf`.Vous trouverez dans les sections ci-dessous quelques uns des paramètres réglables de cette façon. Ils apparaissent ici dans le même ordre que dans le fichier.

DocumentRoot

Un réglage de base est le `DocumentRoot` ; il s'agit du répertoire dans lequel Apache doit trouver les pages web qui seront fournies par le serveur. Pour l'hôte virtuel par défaut, la valeur est`/srv/www/htdocs` et ne doit normalement pas être modifiée.

Timeout

Indique le laps de temps pendant lequel le serveur attend avant d'indiquer un dépassement de délai pour une demande.

MaxClients

Le nombre maximum de clients qu'Apache peut gérer simultanément. La valeur par défaut est `150` ; cependant, cette valeur peut être insuffisante dans le cas d'un site web très fréquenté.

LoadModule

Les directives `LoadModule` indiquent quels modules doivent être chargés. L'ordre de chargement est indiqué par les modules eux-mêmes. Ces directives indiquent de plus dans quel fichier le module est contenu.

Port

Indique le port sur lequel Apache écoute les demandes. C'est habituellement le port 80, le port standard pour HTTP. Normalement, il est déconseillé de modifier cette valeur. On peut souhaiter faire écouter Apache sur un autre port pour tester une nouvelle version d'un site web. De cette manière, la version fonctionnelle du site web est toujours disponible sur le port standard 80.

Une autre raison est de vouloir ne mettre à disposition les pages que sur un intranet car elle contiennent des informations qui ne sont pas destinées à être diffusées au public. Cela peut se faire en mettant la valeur du port à `8080` et en interdisant tout accès extérieur à ce port avec le pare-feu. Le serveur est alors sécurisé contre tout accès provenant de l'extérieur.

Directory

Cette directive permet de fixer les droits d'accès et autres droitssur un répertoire. Une telle directive existe également pour le `DocumentRoot`. Le nom du répertoire indiqué icidoit toujours être modifié en parallèle avec `DocumentRoot`.

DirectoryIndex

Ce paramètre permet de configurer les fichiers que Apache devra chercher pour compléter une URL où manque le nom du fichier à atteindre. Le réglage par défaut est `index.html`. Par exemple, lorsque l'URL `http://www.exemple.com/sous/repertoire` est appelée par le client et lorsque le répertoire `sous/repertoire` existe dans le répertoire `DocumentRoot` et contient bien un fichier `index.html`, cette page est renvoyée au client par Apache.

AllowOverride

Chaque répertoire à partir duquel Apache fournit des documents peut contenir un fichier permettant, pour ce répertoire, de spécifier des droits d'accès et réglages qui prendront le pas sur les droits globalement configurés et d'autres réglages. Ceux-ci sont appliqués de manière récursive pour le répertoire actuel et ses sous-répertoires jusqu'à ce qu'elles soient modifiées dans un sous-répertoire par un fichier similaire. Cela signifie aussi que de tels réglages sont valables globalement s'ils sont indiqués dans un fichier dans le `DocumentRoot`. Ces fichiers portent généralement le nom de `.htaccess`, mais ce nom peut être modifié comme décrit dans la section AccessFileName page ci-contre.

La directive `AllowOverride` permet de définir si les réglages indiqués dans les fichiers locaux pourront remplacer les réglages globaux. Les valeurs possibles sont `None`, `All` ainsi que toutes les combinaisons possibles d'`Options`, de `FileInfo`, de `AuthConfig` et de `Limit`. La documentation d'Apache donne une description précise de la signification de ces valeurs. Le réglage par défaut (sans risque) est `None`.

Order

Cette option a une influence sur l'ordre dans lequel les réglages des droits d'accès `Allow` et `Deny` seront appliqués. L'ordre par défaut est :

```
Order allow,deny
```

Sont d'abord appliqués les droits d'accès pour les accès autorisés et ensuite les droits pour les accès non autorisés. Il y a deux façons d'envisager les droits :

allow all autoriser tout accès, mais en définissant des exceptions.

deny all refuser tout accès, mais en définissant des exceptions.

Exemple pour `deny all`:

```
Order deny,allow
Deny from all
Allow from exemple.com
Allow from 10.1.0.0/255.255.0.0
```

AccessFileName

On peut régler ici le nom des fichiers qui, dans des répertoires servis par Apache, pourront écraser les réglages globaux des droits d'accès et 'autres réglages (voir aussi à ce sujet la section AllowOverride page précédente). Le réglage par défaut est `.htaccess`.

ErrorLog

Indique le nom du fichier dans lequel Apache consigne des messages d'erreur. Le réglage par défaut est `/var/log/httpd/errorlog`. Les messages d'erreur pour les hôtes virtuels (voir la section 30.9 page 561) sont également consignés dans ce fichier lorsqu'aucun fichier journal particulier n'a été indiqué dans la section `VirtualHost` du fichier de configuration.

LogLevel

Les messages d'erreur sont classés en différents niveaux selon l'urgence. Ce réglage indique le niveau d'urgence à partir duquel les messages sont émis. Un réglage sur un niveau indique l'émission de messages de ce niveau et de messages plus urgents. Le réglage par défaut est `warn`.

Alias

On peut indiquer, grâce à un alias, un raccourci vers un répertoire permettant d'accéder directement à ce répertoire. Ainsi, on peut accéder via l'alias `/manuel/` au répertoire `/srv/www/htdocs/manual` même si le répertoire configuré dans le `DocumentRoot` diffère du répertoire `/srv/www/htdocs` (par contre, l'alias ne change rien si le `DocumentRoot` pointe sur ce répertoire). L'utilisation d'un alias permet d'accéder directement au répertoire correspondant avec `http://localhost/manual`. Pour définir les droits sur le répertoire cible spécifié par une directive `Alias`, il peut être nécessaire d'utiliser une directive `Directory`. Voir la section Directory page 551.

ScriptAlias

Cette instruction ressemble à l'instruction alias. Elle indique en plus que les fichiers du répertoire cible doivent être gérés comme des scripts CGI.

Les Server Side Includes

On peut activer les Server Side Includes qui chercheront des instructions SSI au sein des fichiers exécutables. Cela se fait grâce à l'instruction suivante :

```
<IfModule mod_include.c>
XBitHack on
</IfModule>
```

Pour vérifier qu'un fichier contient des SSI, il suffit de le rendre exécutable par `chmod +x` ⟨*nomfichier*⟩. Il est sinon aussi possible d'indiquer explicitement le type de fichiers devant être examinés à la recherche d'instructions SSI. Cela se fait au moyen de :

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Il n'est pas conseillé d'indiquer ici tout simplement `.html` car Apache analyse alors toutes les pages à la recherche de Server Side Includes (même celles qui n'en contiennent certainement pas), ce qui diminue considérablement la performance. Pour SUSE LINUX, ces deux directives figurent déjà dans le fichier de configuration ; il n'y a doncnormalement rien à régler.

UserDir

A l'aide du module `mod_userdir` et de la directive `UserDir`, vous pouvez indiquer un répertoire dans le répertoire personnel de l'utilisateur, dans lequel celui-ci pourra publier ses fichiers via Apache. On peut le régler dans SuSEconfig par le biais de la variable `HTTPD_SEC_PUBLIC_HTML`. Pour permettre de publier les fichiers, il faut que cette variable soit mise à lavaleur `yes`. Cela amène à la déclaration suivante dans le fichier `/etc/apache2/mod_userdir.conf` qui est interprété par `/etc/apache2/httpd.conf`.

```
<IfModule mod_userdir.c>
UserDir public_html
</IfModule>
```



30.7 Utilisation de Apache

Pour afficher vos propres pages web (statiques) avec Apache, il suffit de placer vos fichiers dans le répertoire approprié. Sous SUSE LINUX, il s'agit de `/srv/www/htdocs`. Il se peut que quelques courtes pages d'exemple y soient déjà installées. Celles-ci servent à vérifier si Apache a été installé et fonctionne correctement. Vous pouvez ensuite écraser ou désinstaller ces pages. Vous installez vos propres scripts CGI dans `/srv/www/cgi-bin` .

Pendant qu'il fonctionne, Apache enregistre des messages dans les fichiers journaux `/var/log/httpd/access_log` ou `/var/log/apache2/access_log`. Ces messages indiquent quelles ressources ont fait l'objet d'une requête et ont été fournies, à quel moment et avec quelle méthode (`GET`, `POST` ...). Les messages d'erreur sont enregistrés dans le fichier `/var/log/apache2`.

30.8 Les contenus dynamiques

Apache offre plusieurs possibilités pour fournir des contenus dynamiques. On entend par contenus dynamiques des pages HTML qui ont été générées à partir de données variables fournies par le client, comme par exemple les moteurs de recherche qui, après saisie d'un ou plusieurs mot clés (éventuellement liés par des opérateurs logiques comme ET ou OU) renvoient une liste de pages contenant ces mots.

Apache propose trois moyens de générer des contenus dynamiques :

Les Server Side Includes (SSI) Il s'agit là d'instructions imbriquées dans une page HTML à l'aide de commentaires spéciaux. Apache interprète le contenu des commentaires et fournit le résultat comme une partie de la page HTML.

L'interface Common Gateway Interface (CGI)
Il s'agit de programmes qui se trouvent dans certains répertoires. Apache transmet à ces programmes des paramètres fournis par le client et renvoie le résultat de ces programmes. Ce type de programmation est relativement simple, en particulier du fait qu'on peut concevoirdes programmes existants en ligne de commande de telle manière qu'ils reçoivent des données d'Apache et qu'ils lui renvoient les résultats.

Modules Apache offre des interfaces permettant d'exécuter tout module comme partie du traitement d'une demande. Apache permet à ces programmes

d'accéder à des informations importantes, comme la requête ou l'en-tête HTTP. Les programmes peuvent ainsi prendre part à la génération de contenus dynamiques aussi bien qu'à d'autres fonctions comme l'authentification. La programmation de tels modules requiert un certain niveau d'expertise. Cette approche a l'avantage de fournir de hautes performances et des possibilités qui vont bien au delà SSI ou même de CGI.

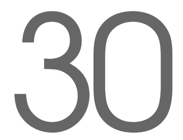
Au contraire des scripts CGI appelés par Apache sous l'identité de leurpropriétaire, les modules sont contrôlés par un interpréteur persistant incorporé à Apache. De cette manière, il n'est pas nécessaire de lancer et d'arrêter un processus séparé pour chaque requête (ce qui entraînerait une charge considérable en gestion de processus, de mémoire, etc.). A la place, le script est géré par l'interpréteur exécuté sous l'identité du serveur web.

Cette approche présente cependant un inconvénient. Comparativement aux modules, les scripts CGI sont relativement robustes face une programmation peu soigneuse. Dans un script CGI, des erreurs comme un oubli de libérer les ressources et la mémoire n'ont pas d'effet à long terme puisque les programmes sont arrêtés après traitement. Ainsi, les ressources non libérées à cause d'une erreur de programmation redeviennent disponibles. Avec des modules, les effets d'erreurs de programmation s'accumulent puisque l'interpréteur fonctionne de façon persistante. Si le serveur n'est pas redémarré et quel'interpréteur fonctionne pendant plusieurs mois, l'incapacité à fournir les ressources demandées, comme par exemple la connexion à une base de données, sont particulièrement désagréables.

30.8.1 Server Side Includes

Les Server Side Includes (SSI) sont des instructions implantées dans des commentaires spéciaux et exécutées par Apache. Leur résultat est inséré dans la sortie. Par exemple, la date actuelle peut être affichée par `<!--#echo var="DATE_LOCAL">`. Ici, c'est le # situé à la suite de la marque d'ouverture de commentaire `<!--` qui indique à Apache qu'il s'agit d'une instruction SSI et non pas d'un commentaire habituel.

Il existe plusieurs possibilités pour activer des SSI. La variante la plus simple consiste à rechercher dans tous les fichiers exécutables des SSI. Une autre variante consiste à définir certains types de fichiers dans lesquels rechercher des SSI. Les deux réglages sont expliquées dans la section Les Server Side Includes page 554.



30.8.2 L'interface Common Gateway Interface : CGI

CGI est l'abréviation de "Common Gateway Interface". Avec CGI, le serveur ne fournit pas seulement une page HTML statique, mais exécute tout un programme qui fournit la page. Il est ainsi possible de créer des pages qui sont le résultat d'un calcul, le résultat d'une recherche dans une base de données. Des arguments peuvent être transmis au programme exécuté, qui est donc à même de fournir une page de réponse individuelle à chaque demande.

CGI a l'avantage d'être une technique assez simple. Il suffit que le programme se trouve dans un certain répertoire pour pouvoir être exécuté par le serveur web exactement comme un programme dans la ligne de commande. Les sorties du programme sur la sortie standard (`stdout`) sont simplement transmises aux clients par le serveur.

En principe, tous les langages de programmation peuvent être utilisés pour écrire des programme CGI. On utilise typiquement des langages de scripts (langages interprétés) comme Perl ou PHP ; dans certains cas, si la vitesse est critique, il peut être plus appropriés d'utiliser C ou C++.

Dans le cas le plus simple, Apache recherche ces programmes dans un répertoire défini (`cgi-bin`). Ce répertoire peut être défini dans le fichier de configuration, décrit dans la section 30.6 page 549. Si nécessaire, il est possible de définir des répertoires supplémentaires. Dans ce cas, Apache pourra y rechercher d'autres programmes exécutables. Cependant, cela comporte un certain risque pour la sécurité puisque tout utilisateur peut faire exécuter par Apache des programmes dont certains peuvent être utilisés avec de mauvaises intentions. Si les programmes exécutables sont restreints au répertoire `cgi-bin`, l'administrateur peut contrôler plus facilement qui y dépose des scripts et des programmes et si ceux-ci sont éventuellement de nature malveillante.

30.8.3 GET et POST

Les paramètres d'entrée sont transmis au serveur par `GET` ou par `POST`. En fonction de la méthode utilisée, le serveur transmet les paramètres au script de différentes manières. Avec `POST`, le serveur transmet les paramètres au programme par l'entrée standard (`stdin`). S'il était démarré sur une console, le programme obtiendrait ses paramètres de la même manière. Avec `GET`, le serveur transmet les paramètres au programme dans la variable d'environnement `QUERY_STRING`.

30.8.4 Générer des contenus dynamiques avec des modules

Apache dispose de nombreux modules. Le terme ”module“ est utilisé avec deux significations. Il existe d'une part des modules qui peuvent être intégrés dans Apache où ils assurent des fonctions précises, tels que les modules décrits ici pour l'utilisation de langages de programmation dans Apache.

D'autre part, dans le contexte de langages de programmation, on comprend par modules un groupe indépendant de fonctions, de classes et de variables. Ces modules sont implantés dans un programme pour proposer certaines fonctionnalités. On peut citer comme exemple les modules CGI existant dans tous les langages de scripts qui facilitent l'écriture d'application CGI en fournissant, entre autres, des méthodes pour lire les paramètres de requête et pour afficher du code HTML.

30.8.5 mod_perl

Perl est un langage de script populaire et ayant fait ses preuves. Pour Perl, il existe une grande quantité de modules et de bibliothèques, dont une bibliothèque pour l'extension du fichier de configuration d'Apache. Vous trouverez un grand choix de bibliothèques pour Perl dans le CPAN (Comprehensive Perl Archive Network— Réseau Complet d'Archive pour Perl) : `http://www.cpan.org/`. `http://www.mongueurs.net/` est un site web en français pour les programmeurs Perl.

Configurer mod_perl

Pour mettre en place `mod_perl` dans SUSE LINUX, il suffit d'installer le paquetage correspondant (voir la section 30.5 page 548). Après l'installation, le fichier de configuration pour Apache contient les déclarations nécessaires (voir `/etc/apache2/mod_perl-startup.pl`). Des informations sur `mod_perl` sont disponibles à l'adresse `http://perl.apache.org/`.

mod_perl comparé à CGI

Dans le cas le plus simple, on peut faire fonctionner un script, jusqu'à présent CGI, en tant que script `mod_perl` en l'appelant à une autre URL. Le fichier de configuration contient des alias, qui font référence au même répertoire et appellent des scripts qu'il contient via CGI ou par `mod_perl`. Toutes ces déclarations figurent déjà dans le fichier de configuration. Pour CGI, la déclaration d'alias est :

```
ScriptAlias /cgi-bin/ "/srv/www/cgi-bin/"
```

Voici les déclarations pour `mod_perl` :

```
<IfModule mod_perl.c>
# Fournit deux alias au même répertoire cgi-bin
# pour illustrer les effets de deux mod_perl différents
# avec le module Apache::Registry
ScriptAlias /perl/          "/srv/www/cgi-bin/"
# avec le module Apache::Perlrun
ScriptAlias /cgi-perl/      "/srv/www/cgi-bin/"
</IfModule>
```

Les déclarations suivantes sont également requises pour `mod_perl`. Elles figurent déjà dans le fichier de configuration.

```
#
# Si mod_perl est activé, charger les informations de configuration
#
<IfModule mod_perl.c>
Perlrequire /usr/include/apache/modules/perl/startup.perl
PerlModule Apache::Registry

#
# configure le module Apache::Registry pour l'alias /perl
#
<Location /perl>
SetHandler  perl-script
PerlHandler Apache::Registry
Options ExecCGI
PerlSendHeader On
</Location>

#
# configure le module Apache::PerlRun pour l'alias /cgi-perl
#
<Location /cgi-perl>
SetHandler  perl-script
PerlHandler Apache::PerlRun
Options ExecCGI
PerlSendHeader On
</Location>

</IfModule>
```

Ces déclarations créent des alias pour les modes `Apache::Registry` et `Apache::PerlRun`. La différence entre les deux modes est décrite ci-dessous :

Apache::Registry Tous les scripts sont compilés puis gardés dans un cache. Chaque script est utilisé en tant contenu d'un sous-programme. Bien que ce fonctionnement soit intéressant du point de vue performance, il présente l'inconvénient suivant : la programmation des scripts doit être faite très soigneusement puisque les variables et les sous-programmes persistent entre les différents appels. Cela signifie qu'il est nécessaire de réinitialiser les variables afin qu'elles puissent être réutilisées lorsqu'elles sont à nouveau appelées. Par exemple, si on enregistre dans un script de banque en ligne le numéro de carte de crédit d'un client dans une variable, ce numéro pourra être présent lorsque le client suivant utilise cette application et donc appelle le même script.

Apache::PerlRun Les scripts sont recompilés pour chaque requête. Les variables et les sous-programmes sont effacés de l'espace de noms entre les requêtes.(l'espace de noms est l'ensemble des noms de variables et de programmes définis à un moment donné pendant l'existence d'un script). Par conséquent, avec `Apache::PerlRun`, une programmation absolument rigoureuse n'est donc pas nécessaire car toutes les variables sont réinitialisées au lancement du script et elles ne peuvent plus contenir de valeurs provenant des appels précédents. Pour cette raison, `Apache::PerlRun` est plus lent que `Apache::Registry`, mais reste plus rapide qu'un CGI (malgré les similitudes avec CGI) car il n'est pas nécessaire d'appeler un processus séparé pour l'interpréteur.

30.8.6 mod_php4

PHP est un langage de programmation spécialement conçu pour être utilisé avec des serveurs web. Il se distingue d'autres langages, dont les commandes sont enregistrées dans des fichiers à part (script), par le fait que lors de PHP, les commandes sont implantées dans une page HTML (semblable à SSI). L'interpréteur PHP traite les commandes PHP et implante le résultat du traitement dans une page HTML.

Le site web de PHP est disponible à l'adresse `http://www.php.net/`. Pour un site sur PHP en français, consultez `http://www.phpindex.com/`. Le paquetage `mod_php4-core` doit être installé pour que PHP fonctionne. Apache 2 requiert en plus le paquetage `apache2-mod_php4`.

30.8.7 mod_python

Python est un langage de programmation orienté objet qui dispose d'une syntaxe très claire et très lisible. La structure du programme dépend de l'indentation, ce qui est une caractéristique inhabituelle mais pratique. Les blocs ne sont pas définis par des accolades (comme c'est le cas dans C et Perl) ou d'autres séparateurs (comme `begin` et `end`), mais par le niveau d'indentation. Le paquetage à installer est `apache2-mod_python`.

Vous trouverez des informations plus détaillées à l'adresse `http://www.python.org/`. Pour plus d'informations sur `mod_python`, consultez `http://www.modpython.org/`.

30.8.8 mod_ruby

Ruby est un langage de programmation de haut niveau orienté objet, relativement récent, présentant des ressemblances avec certains aspects de Perl et Python et particulièrement approprié pour les scripts. Comme Python, il présente une syntaxe claire et transparente. En revanche, Ruby a adopté des abréviations, appréciées par certains programmeurs et détestées par d'autres. Un exemple d'abréviation est `$.r`, le numéro de la dernière ligne lue à partir du fichier d'entrée. Le concept de base de Ruby ressemble beaucoup à Smalltalk.

Vous trouverez le site web de Ruby à l'adresse `http://www.ruby-lang.org/`. Il existe également un module Apache pour Ruby, dont vous trouverez la page web à l'adresse `http://www.modruby.net/`.

30.9 Les hôtes virtuels

Les hôtes virtuels permettent de configurer plusieurs domaines sur un unique serveur du réseau. On économise ainsi les coûts et le travail d'administration nécessaires à l'installation d'un serveur par domaine. Il existe plusieurs possibilités pour les hôtes virtuels :

- les hôtes virtuels basés sur le nom
- les hôtes virtuels basés sur l'adresse IP
- Faire fonctionner plusieurs instances d'Apache sur un seul ordinateur.

30.9.1 Les hôtes virtuels basés sur le nom

Plusieurs domaines peuvent être gérés par une seule instance d'Apache par le biais des hôtes virtuels basés sur le nom. Il n'est alors pas nécessaire de configurer plusieurs adresses IP pour un ordinateur. Il s'agit de l'alternative la plus simple et la plus populaire. Des raisons pour ne pas utiliser d'hôtes virtuels basés sur le nom sont disponibles dans la documentation d'Apache.

Vous pouvez configurer ce point directement dans le fichier de configuration `/etc/apache2/httpd.conf`. Pour activer des hôtes virtuels basés sur nom, il faut indiquer une directive adéquate. `NameVirtualHost **` est suffisante pour qu'Apache accepte toutes les requêtes entrantes. Vous devez ensuite configurer chaque hôte virtuel :

```
<VirtualHost *>
    ServerName www.exemple.com
    DocumentRoot /srv/www/htdocs/exemple.com
    ServerAdmin webmaster@exemple.com
    ErrorLog /var/log/apache2/www.exemple.com-error_log
    CustomLog /var/log/apache2/www.exemple.com-access_log common
</VirtualHost>

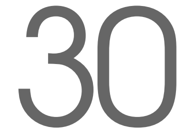
<VirtualHost *>
    ServerName www.monautreentreprise.fr
    DocumentRoot /srv/www/htdocs/monautreentreprise.fr
    ServerAdmin webmaster@monautreentreprise.fr
    ErrorLog /var/log/apache2/www.monautreentreprise.fr-error_log
    CustomLog /var/log/apache2/www.monautreentreprise.fr-access_log common
 </VirtualHost>
```

Une déclaration `VirtualHost` d'hôte virtuel doit également être configurée pour le domaine hébergé par le serveur à l'origine (`www.exemple.com`). Dans cet exemple, le domaine initial et un domaine additionnel (`www.monautreentreprise.fr`) sont hébergés sur le même serveur.

Dans les directives `VirtualHost`, on trouve un *, tout comme pour `NameVirtualHost`. Apache établit le rapport entre la demande et l'hôte virtuel par le champ d'hôte dans l'en-tête HTTP. La demande est transmise à l'hôte virtuel, dont le `ServerName` (nom de serveur) correspond au nom de l'hôte indiqué dans ce champ.

Dans les directives `ErrorLog` et `CustomLog`, il n'est pas crucial que fichiers contiennent le nom du domaine ; on peut utiliser des noms quelconques.

`Serveradmin` désigne l'adresse e-mail de la personne responsable du serveur que l'on peut contacter en cas de problèmes. Si des erreurs se produisent, Apache indique cette adresse dans les messages d'erreur qu'il restitue au client.



30.9.2 Les hôtes virtuels basés sur l'adresse IP

Cette alternative nécessite de configurer plusieurs adresses IP sur l'ordinateur. Une instance d'Apache commande ensuite plusieurs domaines, chaque domaine se voyant attribuer une adresse IP. L'exemple qui suit montre comment configurer Apache afin qu'il héberge, outre sur son adresse IP d'origine `192.168.1.10`, deux autres domaines sur des adresses IP supplémentaires (`192.168.1.20` et `192.168.1.21`). Cet exemple concret ne fonctionne bien sûr que dans un intranet, puisque les adresses IP allant de `192.168.0.0` à `192.168.255.0` ne sont pas routées sur l'Internet.

Configurer les alias IP

Pour qu'Apache puisse héberger plusieurs adresses IP, l'ordinateur sur lequel Apache fonctionne doit accepter les demandes pour plusieurs adresses IP, ce qu'on appelle le Multi-IP-Hosting. Cela nécessite d'abord que les alias IP soient activés dans le noyau, ce qui est le cas par défaut sous SUSE LINUX.

Une fois que le noyau est configuré pour prendre en charge les alias IP, on peut affecter plusieurs adresses IP à l'ordinateur en utilisant les commandes `ifconfig` et `route`. Ces commandes doivent être exécutées en tant qu'utilisateur `root`. On suppose, dans l'exemple suivant, que l'ordinateur dispose déjà de sa propre adresse IP, `192.168.1.10` étant attribuée au périphérique réseau `eth0`.

On peut voir quelle adresse IP est utilisée par l'ordinateur en saisissant la commande `ifconfig`. Pour ajouter d'autres adresses IP, utilisez la commande suivante :

```
ip addr add 192.168.1.20/24 dev eth0
```

Toutes ces adresses IP sont attribuées au même périphérique réseau physique (`eth0`).

Hôtes Virtuels avec adresses IP

Lorsque les alias IP ont été configurés sur le système ou bien que l'ordinateur a été configuré avec plusieurs cartes réseau, on peut procéder à la configuration d'Apache. Indiquez pour chaque serveur virtuel son propre bloc `VirtualHost` :

```
<VirtualHost 192.168.1.20>
    ServerName www.monautreentreprise.fr
    DocumentRoot /srv/www/htdocs/monautreentreprise.fr
    ServerAdmin webmaster@monautreentreprise.fr
    ErrorLog /var/log/apache2/www.monautreentreprise.fr-error_log
    CustomLog /var/log/apache2/www.monautreentreprise.fr-access_log common
</VirtualHost>

<VirtualHost 192.168.1.21>
    ServerName www.encoreuneentreprise.fr
    DocumentRoot /srv/www/htdocs/encoreuneentreprise.fr
    ServerAdmin webmaster@encoreuneentreprise.fr
    ErrorLog /var/log/apache2/www.encoreuneentreprise.fr-error_log
    CustomLog /var/log/apache2/www.encoreuneentreprise.fr-access_log common
</VirtualHost>
```

On n'indique ici les directives `VirtualHost` que pour les domaines supplémentaires ; le domaine initial (`www.exemple.com`) est toujours configuré par les réglages correspondants (`DocumentRoot` etc.) en dehors des blocs `VirtualHost`.

30.9.3 Instances multiples d'Apache

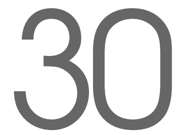
Avec les méthodes précédentes de gestion des hôtes virtuels, les administrateurs d'un domaine peuvent lire les données contenues des autres domaines. Pour séparer les différents domaines les uns des autres, on peut lancer plusieurs instances d'Apache qui utilisent chacune dans le fichier de configuration leurs propres réglages pour `User`, `Group` etc..

Indiquez dans le fichier de configuration pour la directive `Listen` l'adresse IP gérée par l'instance d'Apache correspondante. Comme dans l'exemple précédent, la directive pour la première instance d'Apache serait :

```
Listen 192.168.1.10:80
```

Pour les deux autres instances, elle serait :

```
Listen 192.168.1.20:80
Listen 192.168.1.21:80
```



30.10 Sécurité

30.10.1 Limiter les risques

Si sur un ordinateur, aucun serveur web n'est nécessaire, il vaut mieux désactiver Apache dans l'éditeur de niveaux d'exécution, le désinstaller, ou ne pas l'installer du tout. Afin de minimiser les risques, désactivez tout serveur non utilisé. Cela vaut en particulier pour les ordinateurs qui servent de pare-feu. Si possible, il est vivement recommandé de ne pas faire fonctionner de serveur web sur ces ordinateurs.

30.10.2 Les droits d'accès

DocumentRoot devrait appartenir à root

Le répertoire `DocumentRoot` (`/srv/www/htdocs`) et le répertoire CGI appartiennent par défaut à l'utilisateur `root`. Il n'est pas conseillé de modifier ce paramétrage. Si tout le monde peut écrire dans ces répertoires, il est également possible à tout utilisateur d'y enregistrer des fichiers. Ces fichiers sont ensuite exécutés par Apache avec les droits de l'utilisateur `wwwrun`. De plus, Apache ne doit avoir aucun droit d'écriture sur les données et les scripts qu'il fournit. C'est la raison pour laquelle ceux-ci ne doivent pas appartenir à l'utilisateur `wwwrun`, mais, par exemple, à `root`.

Pour permettre à des utilisateurs de placer des fichiers dans le répertoire de documents d'Apache, il ne faut pas donner les droits d'écriture à tous les utilisateurs. Au lieu de cela, créez un sous-répertoire dans lequel tout le monde peut écrire, comme `/srv/www/htdocs/divers`.

Publier des documents à partir de son propre répertoire personnel

Si les utilisateurs sont autorisés à publier des fichiers, il est possible de déclarer un sous-répertoire de leur répertoire personnel `home` respectif apte à la publication de fichiers. Ce sous-répertoire est traditionnellement nommé `~/public_html`. Cette possibilité est activée par défaut dans SUSE LINUX. Plus de détails sont disponibles en la section UserDir page 554.

On peut alors utiliser sur ces pages l'identité de l'utilisateur dans l'URL. L'URL contient l'élément ~ `nom d'utilisateur` comme raccourci vers le répertoire respectif du répertoire personnel de l'utilisateur. Par exemple, lorsque l'on saisit l'URL `http://localhost/~tux` dans un navigateur, les données du répertoire `public_html` du répertoire personnel de l'utilisateur tux sont affichées.

30.10.3 Toujours rester à la page

Tous ceux qui mettent en place un serveur web, et en particulier si ce serveur web est accessible au public, devraient veiller à rester à la pointe de l'information en ce qui concerne les bogues et les points de vulnérabilité potentiels. Une liste de sources sur les failles exploitables et les correctifs est donnée dans la section 30.12.3 page ci-contre.

30.11 Résolution de problèmes

Si vous rencontrez des problèmes, si Apache n'affiche pas bien, voire pas du tout, une page, les procédures suivantes peuvent vous aider à découvrir la cause du problème. Consultez d'abord le journal des erreurs pour savoir si les messages vous indiquent le problème. Le fichier journal général des erreurs est `/var/log/apache2/error_log`.

Faites défiler, si possible dans une console, les fichiers journaux pour pouvoir voir en parallèle les accès au serveur et la manière dont il réagit. Pour cela, indiquez dans une console `root` la commande suivante :

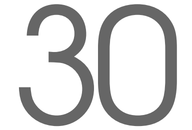
```
tail -f /var/log/apache2/*_log
```

Consultez la base de données des bogues à l'adresse `http://bugs.apache.org/`. Lisez les listes de discussion et les forums. La liste de discussion pour les utilisateurs se trouve à l'adresse `http://httpd.apache.org/userslist.html`. Nous conseillons le forum `comp.infosystems.www.servers.unix` et les forums apparentés.

Si aucune des solutions précédentes n'a résolu votre problème et si vous êtes sûr d'avoir trouvé un bogue dans Apache, adressez-vous directement à nous à l'adresse `http://www.suse.de/feedback/`.

30.12 Documentation complémentaire

Apache est un serveur très utilisé. Vous trouverez donc énormément de documentation à son sujet et de nombreux sites web qui offrent aide et assistance.



30.12.1 Apache

Apache est fourni avec une documentation détaillée. La section 30.5 page 548 décrit comment l'installer. Après installation, la documentation est alors à votre disposition à l'adresse `http://localhost/manual`. La documentation la plus récente est toujours disponible sur le site web d'Apache : `http://httpd.apache.org`

30.12.2 CGI

Pour de plus amples informations sur CGI, consultez les pages suivantes :

- `http://apache.perl.org/`
- `http://perl.apache.org/`
- `http://www.modperl.com/`
- `http://www.modperlcookbook.org/`
- `http://www.fastcgi.com/`
- `http://www.boutell.com/cgic/`

30.12.3 Sécurité

Vous trouverez en permanence à l'adresse `http://www.novell.com/linux/security/securitysupport.html` les correctifs les plus récents pour les paquetages SUSE LINUX. Consultez régulièrement cette URL à partir de laquelle vous pouvez aussi vous abonner à la liste de diffusion "SUSE Security Announcements" (Annonces de SUSE relatives à la sécurité)

L'équipe d'Apache mène une politique d'information ouverte en ce qui concerne les erreurs possibles dans Apache. Vous trouverez des messages actuels sur les bogues et des points d'attaque pouvant éventuellement en résulter à l'adresse `http://httpd.apache.org/security_report.html`. Si vous avez vous-même relevé un problème concernant la sécurité (vérifiez d'abord sur les pages ci-dessus s'il s'agit vraiment d'un problème inconnu), vous pouvez le signaler par courrier électronique à `security@suse.de` ou bien au moyen de `security@apache.org`.

30.12.4 Autres sources

En cas de difficultés, vous pouvez consulter toujours la base de données d'assistance de SUSE `http://portal.suse.com/sdb/en/index.html`. Un

journal publié en ligne, spécialisé sur Apache, est disponible à l'adresse http://www.apacheweek.com/.

L'histoire d'Apache est disponible à l'adresse http://httpd.apache.org/ABOUT_APACHE.html. Vous pourrez également y apprendre pourquoi le serveur s'appelle Apache.

Vous trouverez des informations relatives à la mise à niveau de la version 1.3 vers la version 2.0 sur le site http://httpd.apache.org/docs-2.0/de/upgrading.html.

Synchronisation des fichiers

De nos jours, nombreux sont ceux qui utilisent plusieurs ordinateurs : un ordinateur à la maison, un ou plusieurs ordinateurs sur le lieu de travail et éventuellement en plus un ordinateur portable ou un assistant personnel pour les déplacements. On a besoin d'une grande quantité de fichiers sur tous ces ordinateurs et il est important de pouvoir travailler avec n'importe quel ordinateur, modifier ces fichiers et disposer de leur version la plus récente sur tous les ordinateurs.

31.1 Logiciels pour la synchronisation des données

Sur des ordinateurs reliés en permanence entre eux par un réseau rapide, la synchronisation de fichiers ne pose aucun problème. Dans ce cas, ill suffit de choisir un système de fichiers réseau, comme NFS et d'enregistrer les fichiers sur un serveur. Ensuite, tous les ordinateurs accèdent aux mêmes données par l'intermédiaire du réseau. Cette méthode ne fonctionne pas dans le cas d'une mauvaise connexion réseau ou si la liaison n'est pas permanente. Les personnes qui voyagent avec un ordinateur portable sont amenées à avoir des copies de tous les fichiers sur le disque dur local. Mais lorsque les fichiers sont modifiés, le problème de la synchronisation se pose vite. Si un fichier a été modifié sur un ordinateur, il faut veiller à actualiser aussi la copie du fichier sur tous les autres ordinateurs. Si cette situation ne se produit que de temps en temps, les procédures de copie manuelle à l'aide de scp ou de rsync sont suffisantes. Avec une plus grande quantité de données, la tâche se complique rapidement et requiert une grande attention de la part de l'utilisateur pour éviter des erreurs, comme le remplacement d'une nouvelle version d'un fichier par une version plus ancienne.

Avertissement

Risque de perte de données

Il faut de toute façon se familiariser avec le logiciel utilisé et tester ses fonctions avant de gérer ses données à l'aide d'un système de synchronisation. Pour les données importantes, une sauvegarde est indispensable.

Avertissement

Pour s'épargner le travail fastidieux de la synchronisation manuelle des données comportant, en outre, un risque élevé d'erreurs, il existe des logiciels qui automatisent cette tâche en se basant sur différentes méthodes. Les brefs aperçus suivants ont pour but de donner à l'utilisateur une idée de fonctionnement et de l'utilisation de ces logiciels. Avant de les mettre en œuvre réellement, il vaut mieux lire attentivement la documentation y afférant.

31.1.1 Unison

Dans le cas d'Unison, il ne s'agit pas d'un système de fichiers réseau. Ici, en revanche, on enregistre les fichiers et on travaille avec ces derniers tout à fait nor-

malement en local. Le programme Unison peut être appelé manuellement pour synchroniser des fichiers. Lors de la première synchronisation, une base de données est créée sur les deux ordinateurs concernés, dans laquelle sont enregistrés les sommes de contrôle, les pointeurs temporels et les autorisations des fichiers sélectionnés. Lors de l'appel suivant, unison peut reconnaître quels fichiers ont été modifiés et en proposer la transmission d'un ordinateur vers l'autre. En règle générale, on peut accepter toutes les propositions.

31.1.2 CVS

Utilisé en général pour la gestion de versions de textes sources de logiciels, CVS offre la possibilité de disposer des copies de fichiers sur plusieurs ordinateurs. Il se prête donc parfaitement à ce que nous recherchons. Dans le cas de CVS, il existe une base de données centrale (repository, ou en français, un référentiel) sur le serveur qui ne stocke pas seulement les fichiers mais également les modifications de ces fichiers. Toute modification effectuée localement est validée (commit) dans la base de données pour être reprise (update) par d'autres ordinateurs. Les deux procédures doivent être préparées par l'utilisateur.

En ce qui concerne les modifications, CVS est très tolérant vis-à-vis des erreurs : les modifications sont rassemblées, et il n'y a conflit que si des modifications ont été apportées aux mêmes lignes. Dans ce cas, la base de données reste dans un état stable, le conflit est visible et doit être résolu sur l'ordinateur client.

31.1.3 subversion

Contrairement à CVS qui "a évolué", subversion est un projet développé de façon consistante ; subversion a été créé pour remplacer avantageusement CVS d'un point de vue technique.

Il est clair que subversion apporte une amélioration à CVS dans de nombreux domaines. En raison de son histoire, CVS ne gère que les fichiers et ignore tout des répertoires. Dans subversion, au contraire, les répertoires possèdent aussi un historique de versions et peuvent également être copiés et renommés exactement comme les fichiers. En outre, il est possible d'ajouter à chaque fichier et à chaque répertoire des métadonnées qui sont également soumises à la gestion des versions. À la différence de CVS, subversion offre un accès réseau transparent grâce à quelques protocoles comme WebDAV (Web-based Distributed Authoring and Versioning). WebDAV étend la fonctionnalité du protocole HTTP pour permettre l'accès en écriture en collaboration aux fichiers sur les serveurs web distants.

La réalisation de subversion s'est en grandes parties basées sur des applications existantes. Pour cette raison, le serveur web Apache et l'extension WebDAV sont toujours utilisés en conjonction avec subversion.

31.1.4 mailsync

Comparé aux outils de synchronisation mentionnés jusque-là, mailsync sert uniquement à la synchronisation des messages électroniques entre les différentes boîtes aux lettres. Il peut s'agir aussi bien des fichiers de boîtes aux lettres locaux que de ceux des boîtes aux lettres hébergées sur un serveur IMAP.

Il est décidé, en fonction de l'identificateur de message (message ID) contenu dans l'en-tête du message électronique, individuellement pour chaque message s'il doit être sychronisé ou effacé. Une synchronisation est possible autant entre les différentes boîtes aux lettres qu'entre les hiérarchies de boîtes aux lettres.

31.1.5 rsync

Lorsque vous n'avez pas besoin du contrôle de versions mais que vous souhaitez synchroniser de grandes arborescences de fichiers sur des connexions réseau lentes, l'outil rsync est fait pour vous. rsync dispose de mécanismes minutieux pour transférer exclusivement des modifications dans les fichiers. Cela ne concerne pas seulement les fichiers texte, mais également les fichiers binaires. Pour reconnaître les différences entre fichiers, rsync répartit les fichiers en blocs et calcule des sommes de contrôle correspondant à ces blocs.

L'effort consenti à reconnaître les modifications a aussi un prix. Pour que rsync fonctionne, il faut redimensionner généreusement les ordinateurs qui doivent être synchronisés. Il n'est surtout pas question d'économiser sur la mémoire vive (RAM).

31.2 Critères de choix du logiciel

31.2.1 Comparaison client-serveur et pair à pair

Deux modèles différents de distribution des données sont répandus. Dans le premier modèle, tous les ordinateurs (appelés clients) synchronisent leurs données

avec un serveur central. Le serveur doit être accessible à tous les clients au moins de temps en temps. Ce modèle est utilisé par subversion, CVS et WebDAV.

Dans l'autre modèle, tous les ordinateurs connectés par le réseau peuvent synchroniser mutellement leurs données en tant que pairs. Cette méthode est utilisée par unison. rsync fonctionne en réalité en mode client, mais on peut utiliser chaque client en tant que serveur.

31.2.2 Portabilité

Subversion, CVS et unison sont également disponibles sur de nombreux autres systèmes d'exploitation comme les autres Unix et sous Windows.

31.2.3 Comparaison des modes Interactif et automatique

Dans le cas de subversion, de CVS, de WebDAV et de unison, la synchronisation de données est lancée manuellement par l'utilisateur. Ce comportement permet de contrôler plus précisément les données à synchroniser et de gérer plus aisément les conflits. En revanche, si la synchronisation est réalisée trop rarement, les risques de conflit sont augmentés.

31.2.4 Conflits : apparition et solutions

Dans le cas de subversion ou de CVS, il est rare qu'un conflit survienne, même si plusieurs personnes collaborent pour un même gros projet logiciel. Ceci est dû au fait que les documents sont vérifiés ligne par ligne. En cas de conflit, cela ne concerne toujours qu'un seul client. Un conflit est en principe facile à résoudre avec subversion ou CVS.

Dans le cas d'unison, vous êtes informé des conflits et il est possible d'éviter la synchronisation du fichier. En revanche, les modifications ne sont pas aussi faciles à effectuer qu'avec subversion ou CVS.

Alors que dans subversion ou CVS il est également possible d'enregistrer partiellement des modifications en cas de conflit, WebDAV ne procède à la validation que si l'ensemble de la modification réussit.

rsync n'offre aucun moyen de traiter les conflits. L'utilisateur doit veiller lui-même à ne pas écraser des fichiers par erreur et à résoudre à la main tous les conflits susceptibles d'apparaître. Pour ne pas courir de risques, on peut utiliser aussi un système de contrôle de versions comme RCS.

31.2.5 Sélectionner et ajouter des fichiers

Dans la configuration par défaut d'Unison, toute la structure arborescente du répertoire est synchronisée. Les nouveaux fichiers qui s'y présentent sont automatiquement concernés par la synchronisation.

Avec subversion ou CVS, les nouveaux répertoires et fichiers doivent être ajoutés explicitement au moyen de `svn add` et `cvs add` respectivement. Ceci permet un contrôle précis des fichiers à synchroniser. En revanche, de nouveaux fichiers sont souvent négligés, surtout si, à cause du nombre important de fichiers, les points d'interrogation affichés par `svn update` et `svn status` ou `cvs update` sont ignorés.

31.2.6 Historique

Subversion et CVS offrent une fonctionnalité supplémentaire qui permet la reconstitution des anciennes versions de fichiers. Lors de chaque modification, il est possible d'ajouter une brève note de travail, permettant de suivre ensuite facilement le développement des fichiers grâce au contenu et aux annotations. Ceci constitue une aide très utile pour les projets de fin d'études et les textes de logiciels.

31.2.7 Volume de données et espace disque dur

On a besoin sur tous les ordinateurs concernés de suffisamment d'espace libre sur le disque dur pour héberger toutes les données réparties. Dans le cas de subversion et de CVS, il faut en plus prévoir de l'espace sur le serveur pour la base de données du référentiel. L'historique des fichiers étant également enregistré sur le serveur, l'espace nécessaire est encore plus important. Pour les fichiers au format texte, la place occupée est relativement raisonnable car seules les lignes modifiées sont à nouveau enregistrées. En revanche, pour les fichiers binaires, l'encombrement augmente à chaque modification de la taille du fichier.

31.2.8 GUI, interface utilisateur graphique

Unison offre une interface utilisateur graphique qui affiche les procédures de synchronisation qu'Unison veut réaliser. Vous pouvez accepter la proposition ou rejeter certains fichiers de la synchronisation. En mode texte, il est en outre possible de confirmer individuellement les procédures de façon interactive.

Les utilisateurs expérimentés exécutent normalement subversion ou CVS à la ligne de commande. Il existe cependant des interfaces graphiques pour Linux, telles que cervisia ainsi que pour d'autres systèmes d'exploitation, comme wincvs. Beaucoup d'outils de développement, tels que kdevelop, et d'éditeurs de texte, tels que emacs, offrent une prise en charge de CVS ou subversion. Ces interfaces frontales permettent bien souvent de résoudre plus facilement les conflits.

31.2.9 Convivialité

Unison et rsync sont assez faciles à utiliser et conviennent également aux débutants. CVS et subversion sont un peu plus complexes. Pour ces derniers, il faut avoir comprendre l'interaction entre le référentiel et les données locales. Les modifications des données doivent tout d'abord être comparées localement avec le référentiel. Les commandes `cvs update` et `svn update` sont prévues à cet effet. Les données doivent alors être renvoyées au référentiel avec les commandes `cvs commit` ou `svn commit`. Une fois qu'on a compris cette procédure, même les débutants peuvent facilement utiliser CVS ou subversion.

31.2.10 Sécurité contre les attaques

Dans le cas idéal, les données devraient être protégées contre l'interception et la manipulation. Unison, CVS, rsync et subversion s'utilisent facilement via ssh (secure shell) et sont ainsi sécurisés contre les attaques de ce genre. Il est préférable de ne exécuter CVS ou Unison via rsh (remote shell). De même, l'accès à CVS par le biais du mécanisme *pserver* est à déconseiller dans les réseaux non sécurisés. Grâce à l'utilisation d'Apache, subversion offre d'origine la sécurité nécessaire.

31.2.11 Sécurité contre la perte de données

Beaucoup de développeurs utilisent CVS depuis longtemps pour gérer leurs projets logiciels ; il est particulièrement stable. En enregistrant l'historique du développement, CVS offre même une protection contre certaines erreurs de l'utilisateur, telles que l'effacement accidentel d'un fichier. Bien que subversion ne bénéficie pas encore d'une aussi grande diffusion que CVS, on l'emploie déjà en productiion, par exemple pour le projet subversion lui-même.

Unison est encore relativement récent mais offre une grande stabilité. Il est toutefois plus sensible aux erreurs de l'utilisateur. Lorsqu'on en a terminé avec la synchronisation de l'effacement d'un fichier, celui-ci est irrémédiablement perdu.

TAB. 31.1: *Fonctionnalités des outils de synchronisation de fichiers : -- = très mauvais, - = mauvais ou non disponible, o = moyen, + = bon, ++ = excellent, x = disponible*

	unison	**CVS/subv.**	**rsync**	**mailsync**
Client/Serveur	égale	C-S/C-S	C-S	égale
Portabilité	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interactivité	x	x/x	x	-
Vitesse	-	o/+	+	+
Conflits	o	++/++	o	+
Sél. de fichiers	Répertoire	Sél./fichier, rép.	Répertoire	Boîte aux lettres
Historique	-	x/x	-	-
Espace disque dur	o	--	o	+
Interf. util.	+	o/o	-	-
Complexité	+	o/o	+	o
Attaques	+(ssh)	+/+(ssh)	+(ssh)	+(SSL)
Perte de donn.	+	++/++	+	+

31.3 Introduction à Unison

Unison convient particulièrement à la synchronsation et au transfert d'arborescence de répertoires complète. La synchronisation est bidirectionnelle et peut être contrôlée par une interface graphique intuitive. Bien entendu, vous pouvez aussi utiliser la version console. Il est également possible d'automatiser la synchronisation. Il n'y aura alors aucune interaction avec l'utilisateur mais ceci est à réserver aux utilisateurs expérimentés.

31.3.1 Conditions nécessaires

Unison doit être installé tant sur le client que sur le serveur. Dans ce contexte, le terme *serveur* désigne un deuxième ordinateur distant (contrairement à CVS, comme décrit dans la section 31.1.2 page 571).

Dans la section suivante, nous nous limiterons à l'utilisation d'Unison avec ssh. Dans ce cas, un client SSH doit être installé sur le client et un serveur SSH sur le serveur.

31.3.2 Utilisation d'Unison

Le principe de base d'Unison est l'association de deux répertoires (*roots*). Cette association est de caractère symbolique, il ne s'agit pas d'une connexion en ligne. Supposons que le répertoire soit conçu de la manière suivante :

Client :	`/home/tux/rep1`
Serveur :	`/home/geeko/rep2`

Ces deux répertoires doivent être synchronisés. Sur le client, l'utilisateur est connu en tant que tux, tandis que sur le serveur il est connu en tant que `geeko`. On veut d'abord tester si la communication entre le client et le serveur fonctionne :

```
unison -testserver /home/tux/rep1 ssh://geeko@server//homes/geeko/rep2
```

Voici les problèmes les plus fréquents :

- les versions d'Unison utilisées sur le client et le serveur ne sont pas compatibles
- le serveur ne permet aucune connexion SSH
- aucun des deux chemins d'accès indiqués n'existe

Si tout se déroule bien, n'utilisez pas l'option `-testserver`. Lors de la synchronisation initiale, Unison ne connaît pas encore la relation entre les deux répertoires et fait donc des propositions pour le sens de transfert des différents fichiers et répertoires. Les flèches de la colonne 'Action' indiquent le sens de transfert. Un point d'interrogation signifie qu'Unison ne peut pas faire de proposition concernant le sens du transfert parce que les deux versions ont été modifiées entre-temps ou sont nouvelles.

Le sens de transfert de chaque enregistrement peut être réglé avec les touches de direction (flèches). Si les sens de transfert de tous les enregistrements indiqués sont corrects, cliquez sur 'Go'.

Le comportement d'Unison (par exemple, si la synchronisation doit s'effectuer automatiquement dans les cas sans équivoque) peut être contrôlé par des paramètres spécifiés en ligne de commande au démarrage du programme. Vous trouverez une liste complète de tous les paramètres dans `unison --help`.

Example 31.1: *Le fichier ~/.unison/example.prefs*

```
root=/home/tux/dir1
root=ssh://wilber@server//homes/wilber/dir2
batch=true
```

Pour chaque liaison, la synchronisation est consignée dans le répertoire utilisateur `~/.unison`. Dans ce répertoire, il est possible d'enregistrer des jeux de configuration tels que `~/.unison/example.prefs`. Pour lancer la synchronisation, il suffit tout simplement d'indiquer le fichier comme paramètre en ligne de commande comme dans : `unison example.prefs`.

31.3.3 Informations complémentaires

La documentation officielle d'Unison est très utile, cette section ne fournira donc qu'une brève introduction. Le manuel complet est disponible à l'adresse `http://www.cis.upenn.edu/~bcpierce/unison/` et dans le paquetage `unison` de SUSE.

31.4 Introduction à CVS

CVS est adapté à la synchronisation s'il s'agit de fichiers individuels fréquemment modifiés et dont le format est un format de fichier tel que texte ASCII ou texte source de programme. L'utilisation de CVS pour la synchronisation de fichiers ayant un autre format, tels que les fichiers JPEG, est possible mais conduit très vite à de grandes quantités de données puisque chaque variante d'un fichier est enregistrée en permanence sur le serveur CVS. En plus, dans de tels cas, la plupart des possibilités offertes par CVS ne peuvent pas être utilisées. L'utilisation de CVS pour synchroniser des fichiers n'est possible que si tous les stations de travail peuvent accéder au même serveur.

31.4.1 Configuration d'un serveur CVS

Le *serveur* est le lieu où se trouvent tous les fichiers valables, notamment la dernière version de chaque fichier. Le serveur peut être un ordinateur de bureau fixe. Il est souhaitable que les données du serveur CVS soient régulièrement intégrées dans une sauvegarde.

Une bonne chose lors de la configuration d'un serveur CVS consiste à permettre à l'utilisateur d'accéder au serveur via SSH. Si, sur ce serveur, l'utilisateur est connu comme `tux` et si le logiciel CVS est installé sur le serveur ainsi que sur le client (ordinateur portable), il faut veiller, du côté du client, à ce que les variables d'environnement suivantes soient configurées :

```
CVS_RSH=ssh CVS_ROOT=tux@server:/repserveur
```

Avec la commande `cvs init`, le serveur CVS est ensuite initialisable du côté du client. Cela ne doit être effectué qu'une seule fois.

Enfin, il faut assigner un nom à la synchronisation. Sur un client, choisissez ou créez un répertoire ne contenant que des données qui seront administrées par CVS (le répertoire peut aussi être vide). Le nom du répertoire est également le nom de la synchronisation. Dans l'exemple présent, le répertoire est appelé `synchome`. Entrez dans ce répertoire et saisissez la commande suivante pour appeler la synchronisation `synchome` :

```
cvs import synchome tux wilber
```

Beaucoup de commandes de CVS requièrent un commentaire. A cet effet, CVS démarre un éditeur (celui qui est défini dans la variable d'environnement `$EDITOR` ou vi si aucun éditeur n'est défini). On peut éviter d'appeler un éditeur en entrant le commentaire à l'avance sur la ligne de commande, comme dans l'exemple suivant :

```
cvs import -m 'ceci est un Test' synchome  tux wilber
```

31.4.2 Utilisation de CVS

A partir de ce moment, il est possible de vérifier le référentiel de synchronisation depuis tous les ordinateurs à l'aide de : `cvs co synchome`. Il en résulte un nouveau sous-répertoire `synchome` sur le client. Si vous réalisez des modifications

que vous voulez transmettre au serveur, entrez dans le répertoire `synchome` (ou dans un des ses sous-répertoires) et saisissez : `cvs commit`

Cela provoque, par défaut, la transmission au serveur de tous les fichiers (et sous-répertoires). Si on ne souhaite transmettre que des fichiers ou répertoires individuels, il faut les spécifier comme suit : `cvs commit fichier1 répertoire1` Avant leur transmission au serveur, il faut ajouter les nouveaux fichiers et répertoires au référentiel avec une commande telle que : `cvs add fichier1 répertoire1` Il faut ensuite les transmettre à l'aide de : `cvs commit fichier1 répertoire1`

Pour changer maintenant de poste de travail, il faut vérifier le référentiel de synchronisation, au cas où cela n'a pas encore été fait lors d'une session antérieure sur le même poste de (voir ci-dessus).

Démarrez la synchronisation avec le serveur avec la commande `cvs update`. Actualisez des fichiers ou répertoires avec `cvs update fichier1 répertoire1`. Pour voir les différences entre les fichiers actuels et les versions enregistrées sur le serveur, utilisez la commande `cvs diff` ou la commande `cvs diff fichier1 répertoire1`. Utilisez `cvs -nq update` pour voir quels fichiers ont été affectés par une mise à jour.

Voici certains des symboles d'état utilisés lors d'une mise à jour :

U La version locale a été mise à jour. Ceci concerne tous les fichiers fournis par le serveur et qui manquent sur le système local.

M La version locale a été modifiée. Si les modifications de la version ont eu lieu sur le serveur, les modifications ont pu être également exécutées localement.

P La version locale a été corrigée avec la version du serveur.

C Le fichier local entre en conflit avec la version actuelle du référentiel.

? Ce fichier n'existe pas dans CVS.

L'état `M` marque un fichier localement modifié. Vous pouvez choisir d'envoyer le fichier local modifié au serveur ou de supprimer le fichier local et de procéder à une nouvelle actualisation. Dans ce cas, le fichier manquant est récupéré sur le serveur. Si vous synchronisez un fichier modifié localement et que ce fichier a été modifié au même endroit par plusieurs utilisateurs, cela peut provoquer un conflit lors d'une mise à jour. Ce cas de figure est marqué par le symbole `C`.

Dans ce cas, examinez le fichier correspondant au niveau des marques de conflits (»> et «<) et choisissez entre les deux versions. Ceci risquant d'être relativement pénible, vous pouvez choisir d'abandonner vos modifications en supprimant le fichier local et en saisissant `cvs up` pour récupérer la version actuelle du fichier sur le serveur.

31.4.3 Informations complémentaires

Cette section n'est qu'une petite introduction aux nombreuses possibilités de CVS. Vous trouverez une documentation plus complète sous :

```
http://www.cvshome.org/
http://www.gnu.org/manual/
```

31.5 Introduction à Subversion

Subversion est un système de contrôle de versions Open Source et est souvent considéré comme le successeur de CVS. Par conséquent, les propriétés déjà présentées de CVS s'appliquent aussi en grande partie à subversion. Il est surtout intéressant si l'on souhaite bénéficier des avantages de CVS sans avoir à en subir les inconvénients. Beaucoup de ces propriétés ont déjà été présentées dans les grandes lignes dans la section 31.1.3 page 571.

31.5.1 Configuration d'un serveur Subversion

La configuration d'un référentiel sur un serveur est une procédure assez simple. Pour cela, subversion fournit un outil d'admnistration. Pour installer un nouveau référentiel, saisissez la commande :

```
svnadmin create /chemin/vers/le/referentiel
```

D'autres options sont disponibles via `svnadmin help`. Contrairement à CVS, subversion n'est pas basé sur RCS mais sur la base de données de Berkeley. Veillez à ne pas installer de référentiel sur des systèmes de fichiers distants tels que NFS, AFS ou Windows SMB. La base de données nécessite les mécanismes de verrouillage POSIX que les systèmes mentionnés ci-dessus ne prennent pas en charge.

Pour examiner le contenu d'un référentiel existant, utilisez la commande `svnlook`.

```
svnlook info /chemin/vers/le/referentiel
```

Pour que différents utilisateurs puissent accéder au référentiel, un serveur doit être configuré. Dans ce cas, on peut avoir recours au serveur web Apache avec WebDAV ou utiliser le propre serveur de subversion, svnserve. Dès que svnserve fonctionne, on peut accéder au référentiel à l'aide de `svn://` ou `svn+ssh://` saisi dans un URL. Le fichier de configuration `/etc/svnserve.conf` vous permet de définir les utilisateurs qui doivent s'authentifier à l'invite de `svn`.

La décision pour Apache ou pour svnserve dépend de nombreux facteurs. Ici, un coup d'œil à l'ouvrage consacré à subversion s'impose. Vous trouverez plus d'informations à ce sujet dans la section 31.5.3 page 584.

31.5.2 Utilisation

Pour accéder à un référentiel Subversion, il existe la commande `svn` (similaire à `cvs`). Si le serveur est correctement configuré (avec un référentiel correspondant), chaque client peut accéder à son contenu à l'aide de l'une des commandes suivantes :

```
svn list http://svn.exemple.com/chemin/vers/le/projet
```

ou

```
svn list svn://svn.exemple.com/chemin/vers/le/projet
```

Grâce à la commande `svn checkout`, vous pouvez enregistrer un projet existant dans le répertoire actuel :

```
svn checkout http://svn.exemple.com/chemin/vers/le/projet nom_du_projet
```

La validation crée un nouveau sous-répertoire `nom_du_projet` sur le client. On peut ainsi mettre en œuvre diverses modifications (ajout, copie, renommage, suppression) :

```
svn add fichier
svn copy ancien_fichier nouveau_fichier
svn move ancien_fichier nouveau_fichier
svn delete fichier
```

Chacune de ces commandes est applicable non seulement à des fichiers, mais aussi à des répertoires. De plus, subversion peut aussi attribuer ce que l'on appelle des propriétés à un fichier ou à un répertoire :

```
svn propset license GPL foo.txt
```

Dans l'exemple précédent concernant le fichier `foo.txt`, la propriété `license` se voit attribuer la valeur `GPL`. Grâce à `svn proplist`, vous pouvez afficher les propriétés :

```
svn proplist --verbose foo.txt
Properties on 'foo.txt':
  license : GPL
```

Enregistrez les modifications sur le serveur avec `svn commit`. Pour qu'un autre utilisateur obtienne vos modifications dans son répertoire de travail, il doit procéder à une synchronisation avec le serveur à l'aide de la commande suivante `svn update`.

À la différence de CVS, l'état d'un répertoire de travail dans subversion peut être affiché *sans* avoir à accéder au référentiel avec la commande `svn status`. Dans ce cas, les modifications locales sont affichées dans cinq colonnes, la première colonne étant la plus importante :

'' Aucune modification

'A' L'objet est à ajouter

'D' L'objet est à supprimer

'M' L'objet a été modifié

'C' L'objet est en situation de conflit

'I' L'objet a été ignoré

'?' L'objet n'est pas soumis au contrôle de versions

'!' L'objet est manquant. Cet indicateur apparaît si l'objet a été supprimé ou déplacé sans utiliser la commande `svn`.

'~' L'objet a été pris en charge comme fichier mais il a été, depuis lors, remplacé par un répertoire ou inversement.

La deuxième colonne indique l'état des propriétés. La signification de toutes les autres colonnes est consultable dans l'ouvrage consacré à subversion.

Utilisez la commande `svn help` pour obtenir la description d'un paramètre ou d'une commande :

```
svn help proplist
proplist (plist, pl): List all properties on files, dirs, or revisions.
usage: 1. proplist [PATH...]
       2. proplist --revprop -r REV [URL]

  1. Lists versioned props in working copy.
  2. Lists unversioned remote props on repos revision.
...
```

31.5.3 Informations complémentaires

Le premier point de référence est la page d'accueil du projet subversion, sur le site `http://subversion.tigris.org`. Après l'installation du paquetage `subversion-doc`, vous trouverez un livre en langue anglaise très intéressant et complet dans le répertoire `file:///usr/share/doc/packages/subversion/html/book.html`. Cet ouvrage est également disponible en ligne à l'adresse `http://svnbook.red-bean.com/svnbook/index.html`.

31.6 Introduction à rsync

rsync s'impose toujours quand il s'agit de transférer régulièrement de grandes quantités de données qui ne changent pas de façon trop considérable. C'est fréquemment le cas lorsqu'on met en place une sauvegarde par exemple. Un autre domaine d'application est ce que l'on appelle les staging servers (serveurs étape). Il s'agit de serveurs qui contiennent les arborescences complètes de serveurs web et qui sont mis en miroir régulièrement sur un serveur web dans une DMZ.

31.6.1 Configuration et utilisation

On peut utiliser rsync dans deux modes différents. D'une part, rsync peut archiver ou copier des fichiers. Pour cela, il suffit de faire appel à un shell distant comme par exemple ssh, sur le système cible. Cependant, rsync peut aussi être utilisé comme un `démon` pour fournir des répertoires au réseau.

L'utilisation principale de rsync n'exige aucune configuration particulière. Grâce à rsync, il est possible de mettre directement en miroir des répertoires complets sur un autre ordinateur. Par exemple, à l'aide de la commande suivante, on peut placer une sauvegarde du répertoire personnel de tux sur un serveur de sauvegarde soleil :

```
rsync -baz -e ssh /home/tux/ tux@soleil:backup
```

Pour restaurer le répertoire, utilisez la commande suivante :

```
rsync -az -e ssh tux@soleil:backup /home/tux/
```

Jusqu'ici, l'utilisation se différencie à peine d'un programme normal de copie comme scp

Afin que rsync puisse exploiter pleinement toutes ses fonctionnalités, il faudra l'utiliser en mode "rsync". Pour ce faire, le démon rsyncd est démarré sur un des ordinateurs. Dans ce cas, rsync doit être configuré dans le fichier `/etc/rsyncd.conf`. Si par exemple, il s'agit d'accéder au répertoire `/srv/ftp` via rsync, il est possible de faire appel au fichier de configuration suivant :

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

Le démon rsyncd doit ensuite être démarré avec `rcrsyncd start`. Le démon rsyncd peut aussi être démarré automatiquement lors du processus d'amorçage. Pour cela, il faut activer ce service dans l'éditeur de niveau d'exécution de YaST ou saisir manuellement la commande `insserv rsyncd`. Il est également possible de démarrer rsyncd à partir de xinetd. Toutefois, ce n'est recommandé que pour les serveurs sur lesquels le rsyncd n'est pas trop souvent sollicité.

Dans notre exemple, un fichier journal est également créé pour toutes les connexions. Celui-ci est enregistré dans `/var/log/rsyncd.log`.

Maintenant, le transfert peut être testé depuis un ordinateur client. Cette opération a lieu à l'aide de la commande suivante :

```
rsync -avz soleil::FTP
```

Cette commande permet de répertorier tous les fichiers présents sur le serveur dans le répertoire `/srv/ftp`. Cette requête est aussi enregistrée dans le fichier journal `/var/log/rsyncd.log`. Pour démarrer le transfert, indiquez un répertoire cible. Pour le répertoire actuel, utilisez ".". Par exemple :

```
rsync -avz soleil::FTP .
```

Par défaut, aucun fichier n'est supprimé lors de la synchonisation avec rsync. Lorsque la suppression doit être imposée, il faut indiquer l'option `--delete` en sus. Pour garantir qu'aucun fichier récent n'est écrasé, on peut indiquer l'option `--update` au lieu de `--delete`. Ainsi, les conflits qui en résultent doivent être résolus manuellement.

31.6.2 Informations complémentaires

Vous trouverez des informations importantes sur rsync dans les pages de manuel `man rsync` et `man rsyncd.conf`. Vous trouverez de la documentation technique sur les principes de fonctionnement de rsync dans `/usr/share/doc/packages/rsync/tech_report.ps`. Pour vous tenir informé sur rsync, vous pouvez consulter le site web du projet à l'adresse `http://rsync.samba.org`.

31.7 Introduction à mailsync

En principe, Mailsync s'utilise pour les trois tâches suivantes :

- La synchronisation de courriers électroniques enregistrés localement avec des courriers électroniques enregistrés sur un serveur.
- La migration de boîtes aux lettres dans un format différent ou vers un autre serveur.
- Le contrôle de l'intégrité d'une boîte aux lettres ou la recherche de doubles.

31.7.1 Configuration et utilisation

Mailsync fait la distinction entre la boîte aux lettres elle-même (appelée *store*) et la liaison entre deux boîtes aux lettres (*channel*). Les définitions de stores et de channels sont enregistrées dans le fichier `~/.mailsync`. Vous trouverez ci-dessous la présentation de quelques exemples de stores.

Voici une définition simple :

```
store saved-messages {
   pat Mail/saved-messages
prefix  Mail/
}
```

Mail/ est un sous-répertoire dans le répertoire personnel (/home) de l'utilisateur qui contient des dossiers de courrier électronique, dont entre autres le dossier saved-messages. En appelant mailsync via la commande mailsync -m saved-messages, vous obtenez un index de tous les messages contenus dans saved-messages. Si la définition suivante est donnée :

```
store localdir {
pat     Mail/*
prefix  Mail/
}
```

la commande mailsync -m localdir affiche une liste de tous les messages qui sont enregistrés sous Mail/. En revanche, la commande mailsync localdir affiche une liste des noms des dossiers. On spécifie un store sur un serveur IMAP ainsi :

```
store imapinbox {
server {mail.edu.harvard.com/user=gulliver}
ref    {mail.edu.harvard.com}
pat    INBOX
}
```

Dans ce cas de figure, seul le dossier principal est adressé sur le serveur IMAP ; un store pour les sous-dossiers ressemble à ceci :

```
store imapdir {
server {mail.edu.harvard.com/user=gulliver}
ref {mail.edu.harvard.com}
pat INBOX.*
prefix  INBOX.
}
```

Si le serveur IMAP supporte des liaisons chiffrées, il faudra modifier la spécification du serveur comme suit :

```
server {mail.edu.harvard.com/ssl/user=gulliver}
```

ou bien, si le certificat serveur n'est pas connu :

```
server {mail.edu.harvard.com/ssl/novalidate-cert/user=gulliver}
```

Le préfixe est expliqué plus tard.

Maintenant, on veut connecter les dossiers se trouvant sous `Mail/` aux sous-répertoires sur le serveur IMAP :

```
channel folder localdir imapdir {
msinfo .mailsync.info
}
```

mailsync utilise le fichier de `msinfo` pour conserver une trace des messages qui ont déjà été synchronisés.

La commande `mailsync dossier` a les conséquences suivantes :

- Le type de boîte aux lettres (pattern) est élargi des deux côtés.
- Le préfixe (prefix) résultant de chaque nom de dossier est éliminé.
- Les dossiers sont synchronisés (ou crées, s'ils n'existaient pas) par paires.

De même façon, le dossier `INBOX.sent-mail` sur le serveur IMAP est synchronisé avec le dossier local `Mail/sent-mail` (à condition de répondre aux définitions ci-dessus). La synchronisation entre les différents dossiers fonctionnent de la manière suivante :

- Si un message existe déjà des deux côtés, il ne se passe rien.
- Si le message manque d'un côté et s'il s'agit d'un nouveau message (non consigné dans le fichier de `msinfo`), il y sera transféré.
- Si le message n'existe que d'un côté et s'il s'agit d'un ancien message (déjà consigné dans le fichier de `msinfo`), il y sera effacé (étant donné qu'il existait auparavant de l'autre côté et qu'il y a été effacé).

Pour savoir d'avance quels messages seront transmis et lesquels seront effacés lors d'une synchronisation, on appelle mailsync avec un "channel" *et* un "store" avec : `mailsync dossier localdir`. Il en résulte une liste de tous les messages qui sont localement nouveaux ainsi qu'une liste de tous les messages qui seraient effacés du côté de IMAP lors d'une synchronisation. De la même façon, la commande `mailsync dossier imapdir` affiche une liste de tous les nouveaux messages du côté de IMAP ainsi qu'une liste de tous les messages qui seraient effacés localement lors d'une synchronisation.

31.7.2 Problèmes éventuels

Dans le cas d'une perte de données, la procédure la plus sûre est d'effacer le fichier de protocole du "channel" correspondant de `msinfo`. Il en résulte que tous

les messages qui n'existent que d'un seul côté sont considérés comme nouveaux et seront transmis lors de la prochaine synchronisation.

Seuls les messages portant un identificateur message sont pris en compte par la synchronisation tandis que ceux n'ayant pas d'identificateur message sont tout simplement ignorés ; ils ne sont ni transmis ni effacés. Un identificateur de message manquant est normalement le résultat de programmes défectueux dans le processus de remise ou de génération du courrier.

Sur certains serveurs IMAP, le dossier principal est appelé par `INBOX` et les sous-dossiers sont appelés par un nom quelconque (contrairement à INBOX et INBOX.name). C'est la raison pour laquelle il n'est pas possible de spécifier un modèle exclusif de sous-dossiers pour de tels serveurs IMAP.

Les pilotes de boîtes aux lettres (c-client) qu'utilise mailsync placent, lorsque les messages ont été transmis sur un serveur IMAP, un drapeau d'état spécial, rendant impossible pour certains programmes de messagerie électronique, comme mutt, de reconnaître qu'un message est nouveau. Désactivez ce drapeau d'état spécial avec l'option `-n`.

31.7.3 Informations complémentaires

Le fichier `README` contenu dans le paquetage `mailsync` contient des informations et conseils supplémentaires. Dans ce contexte, le RFC 2076 ”Common Internet Message Headers“ est particulièrement intéressant.

Samba

Samba permet d'utiliser un ordinateur Unix comme serveur de fichiers ou d'impression pour ordinateurs DOS, Windows et OS/2. Ce chapitre vous introduit aux principes de la configuration Samba et décrit les modules de YaST avec lesquels vous pouvez configurer Samba dans votre réseau.

Aujourd'hui, Samba est devenu un produit extrêmement complet. De ce fait, nous pourrons donner ici uniquement un premier aperçu de ses fonctionnalités. Cependant, vous trouverez des détails dans la documentation numérique qui l'accompagne. Celle-ci est constituée, pour une part, de pages de manuel — pour vous faire une idée du volume, exécutez la commande `apropos samba` — et, pour le reste, de documents et d'exemples que vous trouverez, après avoir installé Samba sur votre système, dans le répertoire `/usr/share/doc/packages/samba`. Vous y trouverez également, dans le sous-répertoire `examples` l'exemple de configuration commenté `smb.conf.SuSE`.

Vous disposez du paquetage `samba` dans sa version 3. Voici quelques-unes des nouveautés notables de ce paquetage :

- Prise en charge d'Active Directory.
- La prise en charge d'Unicode a été considérablement améliorée.
- Les mécanismes d'authentification internes ont complètement été remaniés.
- Meilleure prise en charge du système d'impression Windows 200x et Windows XP.
- Configuration en tant que serveur membre (en anglais, member server) de domaines Active Directory.
- Reprise des domaines NT4 pour migrer d'un domaine NT4 vers un domaine Samba.

Astuce

Migration vers Samba3

Si vous souhaitez migrer de Samba 2.x vers Samba 3, vous devez veiller à certaines particularités. Un chapitre complet est consacré à ce sujet dans l'ensemble des HOWTO relatifs à Samba. Une fois le paquetage `samba-doc` installé, vous trouverez le HOWTO sous `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Astuce

Samba utilise le protocole SMB (Server Message Block) qui est basé sur les services NetBIOS. Suite aux pressions de la société IBM, Microsoft a publié le protocole, ce qui a permis à d'autres éditeurs de logiciels de se connecter également à un domaine Microsoft. Samba fait s'appuyer SMB sur le protocole TCP/IP. En conséquence, le protocole TCP/IP doit être installé sur tous les clients. Nous recommandons d'utiliser exclusivement TCP/IP sur les clients.

NetBIOS est une interface logicielle (API) conçue afin de permettre à différents ordinateurs de communiquer entre eux. C'est dans ce contexte qu'a été conçu un

service de nommage (name service) destiné à permettre l'identification mutuelle des machines. En matière de nommage, il n'existe aucune instance centrale qui serait chargée d'attribuer ou de vérifier les droits. Toute machine sur le réseau peut réserver un nombre quelconque de noms, pour autant qu'ils ne soient pas encore attribués. L'interface NetBIOS peut être implémentée sur différentes architectures réseau. Une implémentation relativement proche du matériel réseau porte le nom NetBEUI. NetBEUI est fréquemment désigné sous le nom NetBIOS. Les protocoles réseau implémentés avec NetBIOS sont IPX (NetBIOS via TCP/IP) de Novell et TCP/IP.

Les noms NetBIOS qui sont également attribués dans l'implémentation de NetBIOS sur TCP/IP n'ont rien à voir avec les noms attribués dans le fichier `/etc/host` ou par DNS. NetBIOS définit un espace de nommage complètement à part. Malgré cela, il est recommandé, afin de simplifier l'administration, d'attribuer au moins aux serveurs des noms NetBIOS correspondant à leurs noms d'hôtes DNS. C'est réglé ainsi par défaut dans les serveurs Samba.

Tous les systèmes d'exploitation majeurs tels que Mac OS X, Windows et OS/2 prennent en charge le protocole SMB. Le protocole TCP/IP doit être installé à cet effet. S'agissant des différents UNIX, Samba offre également un client. Linux comporte en outre un module noyau offrant un système de fichiers SMB, permettant d'intégrer des ressources SMB au niveau du système Linux.

Les serveurs SMB offrent aux clients de l'espace disque se présentant sous la forme de "partages" (shares). Un partage correspond à un répertoire et à tous ses sous-répertoires sur le serveur. Il est exporté sous son propre nom et des clients peuvent y accéder sous ce même nom. Le nom du partage peut être choisi librement—il ne doit pas être identique à celui du répertoire exporté. De la même manière, une imprimante exportée se voit attribuer un nom qui sera utilisé par les clients pour y accéder.

32.1 Configuration du serveur

Dans le cas où vous souhaitez utiliser Samba en tant que serveur, installez le paquetage `samba`. Démarrez les services requis pour Samba à l'aide de la commande `rcnmb start & & rcsmb start` et arrêtez-les à l'aide de la commande `rcsmb stop & & rcnmb stop`.

Le fichier de configuration central de Samba est `/etc/samba/smb.conf`. Ce fichier comporte deux parties logiques distinctes. La section `[global]` comporte la définition des paramètres globaux. La seconde section, intitulée `[share]`,

comporte la définition des différents partages de fichiers et d'imprimantes. Ce mode d'organisation permet de définir les détails des partages soit de manière différenciée, soit avec une portée globale dans la section `[global]`. Le fichier de configuration gagne ainsi en lisibilité.

32.1.1 Section global

Les directives suivantes de la section `[global]` doivent être adaptées en fonction de la configuration de votre réseau afin de permettre à d'autres systèmes d'accéder à votre serveur Samba dans un réseau Windows au moyen de SMB.

workgroup = TUX-NET Le serveur Samba est rattaché à un groupe de travail à l'aide de cette ligne. Remplacez `TUX-NET` par votre groupe de travail ou configurez vos clients avec la valeur choisie ici. Votre serveur Samba est visible dans cette configuration avec son nom DNS dans le groupe de travail choisi, pour autant que le nom choisi n'ait pas encore été attribué. Dans le cas où le nom DNS a déjà été attribué, le nom de serveur peut être défini à l'aide de `netbios name = MONNOM`. Pour obtenir plus de précisions sur ce paramètre, exécutez la commande `man smb.conf`.

os level = 2 Ce paramètre définit si votre serveur Samba doit essayer de faire office de LMB (Local Master Browser) pour son groupe de travail. Il est recommandé d'utiliser une valeur volontairement faible afin d'éviter qu'un réseau Windows ne soit perturbé par un serveur Samba mal configuré. Pour plus de précisions sur cette question importante, reportez-vous aux fichiers `BROWSING.txt` et `BROWSING-Config.txt` dans le sous-répertoire `textdocs` de la documentation du paquetage.

En l'absence de serveur SMB préexistant (par exemple Windows NT ou 2000 Server), lorsque c'est le serveur Samba qui doit conserver une liste de tous les systèmes disponibles dans le réseau local, augmentez la valeur `os level` (par exemple à 65). Votre serveur Samba sera alors choisi comme LMB pour votre réseau local.

Dans le cas où cette valeur est modifiée, vous devez être particulièrement prudent en raison des risques de dysfonctionnement auquel vous exposez un réseau Windows existant. Testez les modifications dans un premier temps dans un réseau isolé ou pendant une période non critique.

Prise en charge wins et serveur wins Si vous avez l'intention d'intégrer le serveur Samba au sein d'un réseau Windows existant comportant déjà un serveur WINS, vous devez utiliser l'option `wins server` en y déclarant l'adresse IP de votre serveur WINS.

Si vos systèmes Windows sont utilisés dans des sous-réseaux séparés mais doivent se voir les uns les autres, vous avez besoin d'un serveur WINS. Pour que votre serveur Samba fasse office de serveur WINS, il convient de déclarer `wins support = Yes`. Assurez-vous absolument que vous n'avez utilisé cette directive que pour un seul serveur Samba du réseau. Les options `wins server` et `wins support` ne doivent jamais être activées ensemble dans votre fichier smb.conf.

32.1.2 Partages

Dans les exemples qui suivent, le lecteur de CD-ROM d'une part, ainsi que les répertoires personnels des utilisateurs (`homes`) des clients SMB d'autre part, sont partagés.

[cdrom] Pour éviter qu'un CD-ROM ne soit partagé par inadvertance, toutes les lignes requises de ce partage sont désactivées à l'aide de mises en commentaires (des points-virgules, en l'occurrence). Dans le cas où vous voulez partager le lecteur de CD-ROM avec Samba, il vous suffit de supprimer les points-virgules dans la première colonne.

Example 32.1: *Partage de CD-ROM*

```
;[cdrom]
;       comment = CD-ROM Linux
;        path = /media/cdrom
;        locking = No
```

`\mbox{[cdrom]}` et `\mbox{comment}`
La ligne `[cdrom]` est le nom du partage visible par tous les clients SMB. La directive `comment` permet d'offrir aux clients une description du partage.

`path = /media/cdrom` L'option `path` permet d'exporter le répertoire `/media/cdrom`.

Ce type de partage est uniquement disponible pour les utilisateurs présents sur le système, en raison de paramètres par défaut volontairement restrictifs. Dans le cas où tout le monde doit pouvoir accéder au partage, il convient d'ajouter la ligne `guest ok = Yes`. Compte tenu de la possibilité offerte à tous les utilisateurs de lire les données, la plus grande prudence est de mise avec cette directive, qui devrait être réservée uniquement à quelques partages choisis. La section `[global]` impose d'être particulièrement prudent.

[homes] Le partage `[home]` est particulièrement important. Dans le cas où l'utilisateur possède un compte valide et son propre répertoire personnel sur le serveur de fichiers Linux, son client peut se connecter sur ce compte en fournissant un identifiant utilisateur et un mot de passe valides.

Example 32.2: *Partage "homes"*

```
[homes]
        comment = Home Directories
        valid users = %S
        browseable = No
        read only = No
        create mask = 0640
        directory mask = 0750
```

[homes] En l'absence de partage explicite avec le nom de partage de l'utilisateur qui souhaite se connecter, un partage dynamique est créé, en raison du partage `[homes]`. Le nom du partage est le même que celui de l'utilisateur.

`valid users = %S` Après établissement de la connexion, le `%S` est remplacé par le nom de partage réel. Comme celui-ci est toujours identique au nom d'utilisateur dans le cas du partage `[homes]`, les utilisateurs autorisés sont uniquement le propriétaire du répertoire de l'utilisateur. Cette possibilité vise à n'autoriser l'accès qu'au propriétaire.

`browseable = No` Ce paramètre masque le partage dans l'environnement réseau.

`read only = No` Dans sa configuration par défaut, Samba interdit l'accès en écriture aux partages exportés avec le paramètre `read only = Yes`. Ainsi, si vous voulez partager un répertoire en écriture, vous devez choisir la valeur `read only = No`. Ce paramétrage est équivalent à `writeable = Yes`.

`create mask = 0640` Les systèmes qui ne sont pas basés sur Windows NT ne connaissent pas le système des privilèges d'accès Unix. De ce fait, il n'est pas possible, en créant des fichiers, de définir les privilèges d'accès à appliquer. Le paramètre `create mask` définit les privilèges d'accès à associer aux fichiers à créer. Cette fonctionnalité n'est disponible que pour les partages auxquels on accède en écriture. Ici, cela signifie concrètement que le propriétaire dispose des droits en lecture et écriture et que les membres du groupe primaire disposent

des droits en lecture. À noter que `valid users = %S` interdit l'accès en lecture même lorsque le groupe dispose des droits en écriture. Ainsi, pour accorder l'accès en lecture/écriture au groupe, la ligne `valid users = %S` doit être désactivée.

32.1.3 Niveaux de sécurité

Le protocole SMB, issu du monde DOS/Windows, se préoccupe directement des problèmes de sécurité. Tout accès à un partage peut être protégé par mot de passe. SMB autorise trois modes de contrôle d'autorisations :

Sécurité au niveau du partage (security = share) :
Dans la sécurité au niveau du partage, un mot de passe est attribué à un partage. Tous ceux qui connaissent ce mot de passe ont accès au partage.

Sécurité au niveau de l'utilisateur (security = user) :
Cette variante introduit le concept de l'utilisateur dans SMB. Chaque utilisateur doit se connecter sur le serveur à l'aide d'un mot de passe. Après la phase d'authentification, le serveur peut ensuite offrir l'accès aux différents partages exportés en fonction du nom d'utilisateur indiqué.

Sécurité au niveau du serveur (security = server) :
Vis-à-vis des clients, Samba affirme travailler en mode sécurité au niveau de l'utilisateur. Il transmet cependant toutes les demandes de mot de passe à un autre serveur en mode sécurité au niveau de l'utilisateur qui assure l'authentification. Cette configuration prévoit un paramètre supplémentaire (`password server =`).

La distinction entre sécurité au niveau du partage, de l'utilisateur et du serveur s'applique au serveur dans son ensemble. Il n'est pas possible d'exporter certains partages d'un serveur configuré pour utiliser la sécurité au niveau du partage et d'autres en utilisant la sécurité au niveau de l'utilisateur. Vous pouvez toutefois exploiter sur un système un serveur Samba différent pour chaque adresse IP configurée.

Pour plus de précisions sur ce sujet, veuillez consulter l'ensemble des HOWTO relatifs à Samba. Si votre système comporte plusieurs serveurs, les paramètres `interfaces` et `bind interfaces only` vous concernent.

Astuce

Le programme swat peut être utilisé pour les tâches simples d'administration du serveur Samba. Celui-ci comporte une interface web simple permettant de configurer aisément le serveur Samba. Appelez dans un navigateur Web l'adresse `http://localhost:901` et connectez-vous en tant qu'utilisateur `root`. Veuillez noter que swat doit également être activé dans les fichiers `/etc/xinetd.d/samba` et `/etc/services`. Vous devez pour cela remplacer dans `/etc/xinetd.d/samba` la ligne `disable` par `disable = no`. Pour plus d'informations relatives à swat, reportez-vous à la page de man de swat.

Astuce

32.2 Samba en tant que serveur de login

Dans les réseaux comportant essentiellement des clients Windows, il est généralement souhaitable de permettre uniquement aux utilisateurs disposant d'un compte et d'un mot de passe valides de se connecter. On peut offrir cette fonctionnalité à l'aide d'un serveur Samba. Dans un serveur basé sur Windows, cette fonction est assurée par le serveur Windows NT qui est configuré comme contrôleur de domaine primaire (Primary Domain Controller ou PDC). Les lignes correspondantes doivent être ajoutées à la section `[global]` de `smb.conf`, comme indiqué dans l'exemple 32.3 de la présente page.

Example 32.3: *Section "global" dans smb.conf*

```
[global]
        workgroup = TUX-NET
        domain logons = Yes
        domain master = Yes
```

Lorsque des mots de passe chiffrés sont utilisés pour la vérification—ce qui est la règle dans les versions correctement maintenues de Windows 9x, Windows NT 4.0 service pack 3 et suivants, et dans tous les systèmes plus récents—le serveur Samba doit être en mesure de les gérer. C'est le rôle de la ligne `encrypt passwords = yes` dans la section `[global]` ; option spécifiée par défaut, à

partir de la version 3 de samba. Parallèlement, les comptes utilisateur ou les mots de passe doivent être chiffrés en utilisant une méthode de chiffrement conforme à Windows. L'opération est réalisée à l'aide de la commande `smbpasswd -a nom`. Dans la philosophie Windows des domaines NT, les machines elles-mêmes ont besoin d'un compte de domaine. Celui-ci est créé à l'aide des commandes suivantes :

Example 32.4: *Création d'un compte de machine*

```
useradd nommachine\$
smbpasswd -a -m nommachine
```

Un signe dollar a été ajouté dans la commande `useradd`. La commande `smbpasswd` l'ajoute elle-même lorsqu'on utilise le paramètre `-m`. Dans la configuration qui nous sert d'exemple (`/usr/share/doc/packages/samba/examples/smb.conf.SuSE`), certains paramètres permettant d'automatiser ces opérations ont été prévus.

Example 32.5: *Création automatique d'un compte de machine*

```
add machine script = /usr/sbin/useradd -g nogroup -c \
"NT Machine Account" -s /bin/false %m\$
```

Pour que ce script puisse être correctement exécuté par Samba, vous avez encore besoin d'un utilisateur Samba détenant les droits d'administrateur. Ajoutez pour ce faire l'utilisateur souhaité au groupe `ntadmin`. Vous pouvez alors ajouter tous les utilisateurs de ce groupe Unix au `Domain Admins` à l'aide de la commande suivante :

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Vous trouverez davantage d'informations à ce sujet dans l'ensemble des HOWTO relatifs à Samba, dans le chapitre 12 sous `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

32.3 Configuration du serveur Samba avec YaST

Démarrez la configuration du serveur en choisissant le groupe de travail ou le domaine qui sera contrôlé par votre nouveau serveur Samba. Sélectionnez un groupe/domaine de travai dans le menu déroulant 'Nom de groupe de travail ou domaine' ou entrez-en un nouveau. Dans l'étape suivante, spécifiez si votre serveur doit agir en tant que contrôleur de domaine principal (PDC, primary domain controller) ou en tant que contrôleur de domaine de secours (BDC, backup domain controller).



FIG. 32.1: *Configuration de Samba—Démarrage*

Dans le menu 'Démarrer' (figure 32.1 de la présente page), activez Samba. Utilisez 'Ouvrir ports dans le pare-feu' et 'Détails du pare-feu', pour adapter le pare-feu fonctionnant sur le serveur de façon à ce que les ports pour les services `netbios-ns`, `netbios-dgm`, `netbios-ssn` et `microsoft-ds` soient ouverts sur toutes les interfaces (externes et internes), permettant ainsi un fonctionnement sans problèmes du serveur Samba.

Dans le menu 'Partages' (figure 32.2 page suivante), définissez quels partages

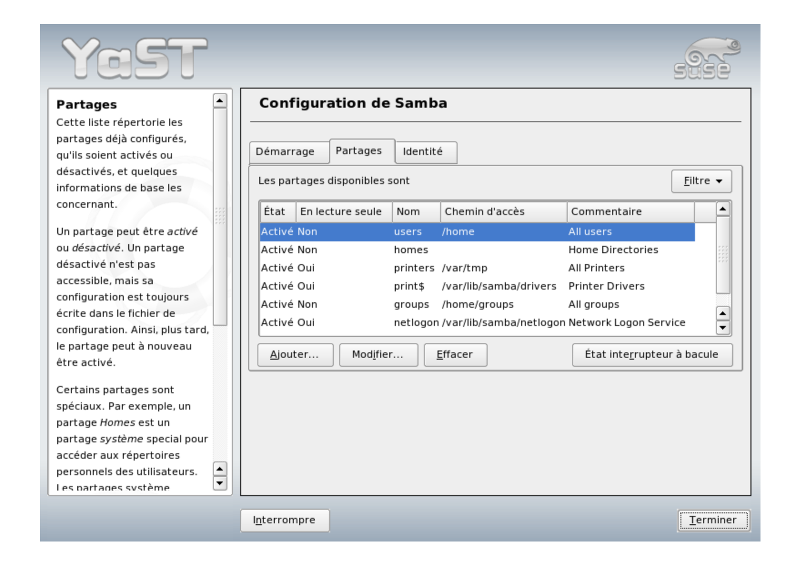


FIG. 32.2: *Configuration Samba—partages*

Samba doivent être activés. Le bouton 'Changer l'état' permet de passer de l'état 'actif' à 'inactif' et vice-versa. Ajoutez de nouveaux partages avec 'Ajouter'.

Dans le menu 'Identité' (figure 32.3 page suivante), définissez à quel domaine l'ordinateur appartient ('Configuration de base') et si vous souhaitez un nom d'ordinateur alternatif dans le réseau ('Nom d'hôte NetBIOS').

32.4 Configuration des clients

Les clients ne peuvent accéder au serveur Samba que par TCP/IP. Les protocoles NetBUI ou NetBIOS via IPX ne peuvent pas être utilisés avec Samba.

32.4.1 Configuration d'un client Samba avec YaST

Configurez un client Samba pour accéder simplement aux ressources (fichiers ou imprimantes) disponibles sur le serveur Samba. Entrez, dans le dialogue 'Groupe de travail Samba', le domaine ou le groupe de travail. Cliquez 'Parcourir' pour

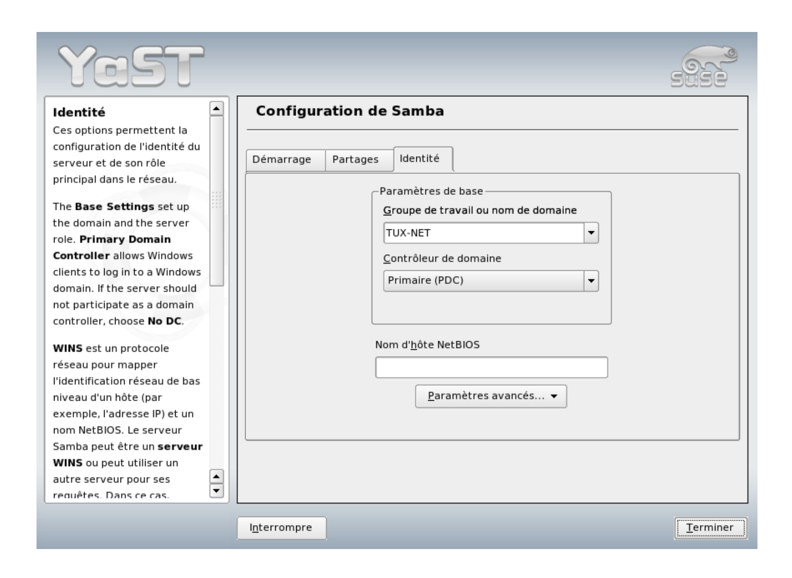


FIG. 32.3: *Configuration Samba-–identité*

afficher tous les groupes et domaines disponibles et qui peuvent être sélectionnés d'un clic de souris. Activez 'Utiliser les informations SMB aussi pour l'authentification Linux' et l'authentification des utilisateurs se fera à l'aide du serveur Samba. Lorsque vous avez procédé au réglage de tous les paramètres, cliquez sur 'Terminer' pour achever la configuration.

32.4.2 Windows 9x et ME

Windows 9x et ME prennent en charge le protocole TCP/IP. Toutefois, celui-ci n'est pas installé dans l'installation par défaut. Pour installer TCP/IP après l'installation du système, allez dans 'Panneau de contrôle' → 'Système' et sélectionnez 'Ajouter' → 'Protocoles' → 'TCP/IP de Microsoft'. Après avoir redémarré la machine Windows, vous pouvez trouver le serveur Samba en double-cliquant sur l'icône de bureau pour l'environnement de réseau.

Astuce

Pour utiliser une imprimante sur un serveur Samba, il convient d'installer le pilote d'imprimante générique ou Apple PostScript correspondant à la version de Windows concernée ; l'idéal est de se connecter avec la file d'attente d'impression Linux qui accepte le format PostScript en entrée.

Astuce

32.5 Optimisation

`socket options` est une optimisation possible fournie avec l'échantillon de configuration qui accompagne votre version de Samba. Ses paramètres par défaut font référence à un réseau local Ethernet. Pour plus de détails au sujet de `socket options`, veuillez vous reporter à la section concernée des pages de manuel de `smb.conf` et à la page de manuel de `socket(7)`. Pour plus d'informations à ce sujet, reportez-vous, dans l'ensemble des HOWTO relatifs à Samba (Samba HOWTO Collection), au chapitre en anglais `Samba performance tuning` (optimisation des performances de Samba).

La configuration par défaut dans `/etc/samba/smb.conf` tente de proposer des valeurs utiles, tout en se basant sur les paramètres par défaut de l'équipe Samba. Pour autant, il n'est pas possible de mettre au point une configuration toute faite surtout en ce qui concerne la configuration du réseau ou du nom du groupe de travail. Vous trouverez, dans le fichier commenté `examples/smb.conf.SuSE` comportant la configuration donnée en exemple, de nombreuses informations complémentaires qui vous aideront à ajuster votre configuration en fonction de vos besoins propres.

Astuce

L'équipe Samba propose, dans la collection de HOWTO Samba, une section consacrée à la recherche d'erreurs. La partie V contient en outre une marche à suivre détaillée pour la vérification de la configuration.

Astuce

Le serveur proxy Squid

Squid est un serveur proxy cache largement répandu pour les plates-formes Linux et UNIX. Cette section explique comment le configurer, les réglages nécessaires pour le faire fonctionner, comment le système à proprement parler doit être configuré pour mettre des fichiers à disposition de manière transparente, la manière d'obtenir des statistiques sur l'utilisation du cache à l'aide de programmes tels que Calamaris et cachemgr et comment filtrer le contenu web avec squidGuard.

33.1 Squid utilisé comme serveur proxy cache

Squid est un serveur proxy cache. Il transmet au serveur les demandes qu'il reçoit des clients (dans ce cas, les navigateurs web). Lorsque les objets demandés arrivent du serveur, il les transmet au client et en garde une copie sur un cache de son disque dur. L'un des avantages de la mise en cache est que plusieurs clients demandant le même objet peuvent obtenir la réponse à partir du cache stocké sur le disque dur. Les clients reçoivent ainsi les données beaucoup plus rapidement que depuis l'Internet. Parallèlement, cela permet d'économiser la bande passante.

Outre la mise en cache (caching), Squid offre un large éventail de fonctionnalités. Il permet, par exemple, de définir des hiérarchies entre serveurs proxy pour permettre de répartir la charge du système, de définir des règles d'accès précises pour l'ensemble des clients qui souhaitent accéder au serveur proxy, d'autoriser ou de refuser l'accès à certaines pages web à l'aide d'autres applications ou d'établir des statistiques sur les pages web les plus consultées pour évaluer le comportement de navigation des utilisateurs. Squid n'est pas un serveur proxy générique. Normalement il ne sert de médiateur qu'entre des connexions HTTP. En outre, il prend en charge les protocoles FTP, Gopher, SSL et WAIS mais ne gère pas les autres protocoles Internet tels que Real Audio, les forums (News) ou les vidéoconférences. Squid n'a recours au protocole UDP que pour assurer la communication entre différents caches. C'est pour cette raison qu'il ne prend pas non plus en charge d'autres programmes multimédia.

33.2 Informations au sujet du serveur proxy cache

33.2.1 Squid et la sécurité

Vous pouvez utiliser Squid conjointement avec un pare-feu pour protéger de l'extérieur les réseaux internes en utilisant un serveur proxy cache. Le pare-feu interdit à tout client, à l'exception de Squid, d'établir une connexion avec des services externes. Toutes les connexions web doivent être établies par l'intermédiaire du serveur proxy.

Dans le cas d'un pare-feu avec une DMZ (zone démilitarisée), installez votre serveur proxy dans cette zone. Il est alors important que tous les ordinateurs de la DMZ n'envoient leurs fichiers de journaux qu'à des ordinateurs à l'intérieur du réseau sécurisé. La possibilité de mettre en place un tel serveur proxy "transparent" est décrite dans la section 33.6 page 618.

33.2.2 Caches multiples

Vous pouvez configurer plusieurs serveurs proxy de manière à ce qu'ils puissent échanger des objets entre eux. Ceci réduit la charge du système et augmente la probabilité de trouver un objet lorsque celui-ci est déjà disponible sur le réseau local. Il est également possible d'établir des hiérarchies de caches, afin qu'un cache soit en mesure soit de faire suivre des demandes d'objets aux caches de même niveau hiérarchique, soit de demander à un cache de niveau supérieur de télécharger les objets à partir d'un autre cache du réseau local ou directement à la source.

Il est important de choisir soigneusement la topologie pour la hiérarchie de caches afin de ne pas augmenter le trafic réseau global. Ainsi, dans un réseau constitué de nombreuses machines, il est possible de configurer un serveur proxy pour chaque sous-réseau, et de lier ensuite celui-ci à un serveur proxy de niveau supérieur, à son tour connecté au serveur proxy cache du fournisseur d'accès à Internet.

Toute la communication est gérée par le protocole ICP (Internet Cache Protocol) placé au-dessus du protocole UDP. L'échange de données entre les caches se fait à l'aide du protocole HTTP (Hyper Text Transmission Protocol) basé sur TCP.

Pour trouver les meilleurs serveurs pour les objets souhaités, un cache envoie une requête ICP à tous les serveurs proxy du même niveau hiérarchique. Les serveurs proxy réagissent alors à ces demandes avec des réponses ICP contenant le code "HIT" si l'objet a été trouvé ou le code "MISS" dans le cas contraire. S'il a obtenu plusieurs réponses HIT, le serveur proxy désigne un serveur particulier pour le téléchargement. La rapidité de réponse d'un cache, ou sa proximité physique, font partie des paramètres de décision. Si la réponse n'est pas satisfaisante, la demande est transmise au cache de niveau supérieur.

Astuce

Pour éviter d'enregistrer plusieurs fois des objets dans différents caches du réseau, d'autres protocoles ICP sont également utilisés, comme par exemple CARP (Cache Array Routing Protocol) ou HTCP (Hyper-Text Cache Protocol). Plus il y a d'objets présents sur le réseau, plus il est facile de trouver celui qui est cherché.

Astuce

33.2.3 Mise en cache d'objets Internet

Tous les objets disponibles sur le réseau ne sont pas statiques. Il existe de nombreuses pages CGI générées de manière dynamique, des compteurs d'accès ou des documents SSL chiffrés pour garantir un certain niveau de sécurité. C'est pour cette raison que ce type d'objets n'est pas conservé en cache : en effet, à chaque nouvel accès, l'objet est modifié.

Pour tous les autres objets qui se trouvent dans le cache, se pose la question de savoir combien de temps ils doivent y rester. Tous les objets sont donc classés dans le cache en fonction de différents critères, afin de pouvoir prendre cette décision. Les en-têtes `Last modified` ("dernière modification") ou `Expires` ("expire le") et la date correspondante permettent aux serveurs web et proxy de s'informer de l'état d'un objet. D'autres en-têtes sont également utilisées pour indiquer par exemple qu'un objet donné ne doit pas faire l'objet d'un enregistrement intermédiaire.

Les objets stockés dans le cache sont généralement remplacés si la place vient à manquer, et ce à l'aide d'algorithmes tels que Last Recently Used (LRU) développés spécialement pour la gestion des objets en cache. Le principe consiste, en substance, à remplacer les objets demandés le moins fréquemment.

33.3 Configuration requise

Vous devez tout d'abord déterminer la charge maximale du système. Ainsi, il est capital d'accorder une attention particulière aux pointes de charge du système, dans la mesure où celles-ci peuvent être plus de quatre fois plus élevées que la moyenne quotidienne. En cas de doute, il est préférable de surévaluer la configuration matérielle requise car un Squid qui fonctionne à sa limite peut entraîner

une perte de qualité de service considérable. Vous allez découvrir dans les sections suivantes les différents facteurs liés au système, classés en fonction de leur importance.

33.3.1 Disques durs

La vitesse joue un rôle déterminant dans le processus de mise en cache. Il convient donc d'accorder une attention toute particulière à ce facteur. Pour les disques durs, ce paramètre est désigné par le *temps d'accès direct*, exprimé en millisecondes. Comme, la plupart du temps, Squid lit ou écrit des blocs de données de petite taille sur le disque dur, le temps d'accès d'un disque dur est plus déterminant que son débit. De ce point de vue, il est particulièrement intéressant de choisir des disques durs ayant une vitesse de rotation élevée, qui permet un positionnement plus rapide de la tête de lecture/écriture à l'endroit voulu. Pour augmenter la vitesse du système, une solution consiste à utiliser simultanément plusieurs disques durs ou à utiliser des matrices de disques entrelacés RAID (Striping Raid Arrays).

33.3.2 Taille du cache du disque dur

Dans un petit cache, la probabilité d'obtenir un HIT (l'objet souhaité est déjà présent) est faible, car le cache peut vite être rempli. Dans ce cas, les objets les moins fréquemment demandés sont remplacés par des nouveaux. Si par exemple le cache dispose d'1 Go et que l'utilisateur n'a besoin que de 10 Mo par jour pour naviguer, il faut donc plus de cent jours pour remplir le cache.

Le plus simple consiste à déterminer la taille du cache en fonction du débit maximal de la connexion. Pour une connexion à 1 Mbit/s, le débit maximal est égal à 125 Ko/s. Si la totalité des données du trafic arrive dans le cache, ceci représente au bout d'une heure un volume de 450 Mo. Si l'on suppose ensuite que le trafic total de données n'est généré que pendant huit heures de travail, on obtient pour une journée 3,6 Go. Comme la connexion n'est généralement pas exploitée jusqu'à sa capacité maximale, on peut en déduire que le volume total de données traitées par le cache s'élève environ à 2 Go. Dans cet exemple, 2 Go d'espace disque sont donc nécessaires à Squid pour conserver en cache toutes les données de toutes les pages consultées en une journée.

33.3.3 Mémoire vive

La quantité de mémoire centrale (RAM) utilisée par Squid dépend directement du nombre d'objets placés en cache. Squid stocke aussi, dans la mémoire centrale, des renvois vers les objets en cache ainsi que les objets fréquemment demandés afin de pouvoir extraire ces données plus rapidement. La mémoire centrale est beaucoup plus rapide qu'un disque dur.

Squid doit conserver également d'autres données en mémoire, par exemple une table de toutes les adresses IP attribuées, un cache de noms de domaines précis, les objets les plus fréquemment demandés, des listes de contrôle d'accès, des tampons, etc.

Il est très important que le processus Squid dispose de suffisamment de mémoire. S'il devait avoir recours à la partition d'échange, les performances du système s'en verraient considérablement réduites. Vous pouvez utiliser l'outil cachemgr.cgi pour gérer la mémoire du cache. Vous en trouverez une présentation dans la section 33.7 page 621.

33.3.4 Processeur

Squid n'a pas besoin d'un processeur très puissant. Ce n'est que lorsque le contenu du cache est chargé ou vérifié que la charge du processeur augmente. L'utilisation d'ordinateurs multiprocesseurs n'augmente pas les performances du système. Pour augmenter l'efficacité, il est plutôt recommandé d'utiliser des disques durs plus rapides ou d'ajouter de la mémoire centrale.

33.4 Démarrer Squid

Sous SUSE LINUX, Squid est déjà préconfiguré de telle sorte que vous pouvez le démarrer dès que l'installation est terminée. L'une des conditions préalables à un démarrage en douceur est que le réseau soit configuré de manière à pouvoir accéder à au moins un serveur de noms et à l'Internet. On peut rencontrer des problèmes lors de l'utilisation d'une connexion distante avec une configuration DNS dynamique. Dans ce cas, au moins le serveur de noms doit être indiqué de manière fixe, car Squid ne démarre pas s'il ne trouve pas de serveur de noms dans `/etc/resolv.conf`.

33.4.1 Commandes pour démarrer et arrêter Squid

Pour démarrer Squid, saisissez sur la ligne de commande, en tant que `root`, la commande `rcsquid start`. La première fois, le script de démarrage `/etc/init.d/squid` crée automatiquement la structure de répertoires dans `/var/squid/cache`, ce qui peut durer de quelques secondes à quelques minutes. Si `done` apparaît à droite en vert, Squid est correctement démarré. Vous pouvez tester le fonctionnement de Squid en déclarant dans le navigateur un serveur proxy à l'adresse `localhost` et sur le port `3128`.

Pour permettre à tous les utilisateurs d'accéder à Squid et, grâce à lui, à l'Internet, vous devez changer dans le fichier de configuration `/etc/squid/squid.conf` la ligne `http_access deny all` en `http_access allow all`. Il ne faut cependant pas oublier qu'en procédant de la sorte vous ouvrez complètement Squid à tout le monde. Partant de ce constat, vous devez définir des ACL (listes de contrôle d'accès) qui réglementent l'accès au serveur proxy. Pour plus d'informations à ce sujet, se reporter à la section 33.5.2 page 616.

Si vous avez modifié le fichier de configuration `/etc/squid/squid.conf`, Squid doit le lire à nouveau. Faites-le avec la commande `rcsquid reload`. Vous pouvez aussi redémarrer Squid complètement avec la commande `rcsquid restart`.

La commande `rcsquid status` vous permet de déterminer si le serveur proxy fonctionne. On arrête Squid avec la commande `rcsquid stop`. L'arrêt peut prendre un certain temps, car Squid attend jusqu'à trente secondes (option `shutdown_lifetime` dans `/etc/squid/squid.conf`) avant d'interrompre les connexions avec les clients et d'écrire ses données sur le disque.

Avertissement

Arrêter Squid

Si vous arrêtez Squid avec `kill` ou `killall`, vous pouvez endommager le cache que vous devrez alors vider pour pouvoir redémarrer Squid.

Avertissement

Si Squid s'arrête peu de temps après avoir démarré correctement, cela peut être dû à un enregistrement de serveur de noms erroné ou à un fichier `/etc/resolv.conf` absent. Squid enregistre la raison de l'échec du démarrage dans le fichier `/var/squid/logs/cache.log`. Si Squid doit être démarré automatiquement lors de l'amorçage, il doit être activé pour les niveaux d'exécution cor-

respondants dans l'éditeur de niveaux d'exécution de YaST. Voir la section 2.7.7 page 80.

Lors d'une désinstallation de Squid, ni la hiérarchie de caches, ni les fichiers journaux ne sont supprimés. Vous devez supprimer manuellement le répertoire `/var/cache/squid` pour les effacer.

33.4.2 Serveur de noms local

Il est cohérent d'utiliser un serveur de noms local même s'il n'a pas à gérer son propre domaine. Il fonctionne alors seulement en tant que serveur de noms cache (caching-only name server) et peut, sans configuration particulière, résoudre les requêtes DNS grâce aux serveurs de noms racine (voir la section 24.2 page 468). La façon de faire dépend de si vous avez choisi ou non le DNS dynamique lors de la configuration de la connexion internet.

DNS dynamique Normalement, avec DNS dynamique, le serveur DNS est défini par le fournisseur lors de l'établissement de la connexion internet et le fichier local `/etc/resolv.conf` est ajusté automatiquement. Ce comportement est obtenu à l'aide de la variable sysconfig `MODIFY_RESOLV_CONF_DYNAMICALLY` à laquelle est attribuée la valeur `YES`. Attribuez la valeur `NO` à cette variable avec l'éditeur sysconfig de YaST (voir la section 7.8 page 180). Entrez alors le serveur DNS local dans le fichier `/etc/resolv.conf` avec l'adresse IP `127.0.0.1` pour `localhost`. De cette façon, Squid peut toujours trouver le serveur de noms local lorsqu'il démarre.

Pour que le serveur de noms du fournisseur soit accessible, son nom doit être entré dans le fichier de configuration `/etc/named.conf` sous `forwarders` avec son adresse IP. Avec le DNS dynamique, ceci peut être effectué automatiquement lors de l'établissement de la connexion à l'aide de la variable sysconfig `MODIFY_NAMED_CONF_DYNAMICALLY` à laquelle doit être attribuée la valeur `YES`.

DNS statique Avec DNS dynamique, aucun ajustement automatique concernant DNS n'est fait lors de l'établissement de la connexiont. Il n'est donc pas nécessaire de changer des variables sysconfig mais vous devez préciser le serveur DNS local dans le fichier `/etc/resolv.conf` comme décrit ci-dessus. Par ailleurs, le serveur de noms statique du fournisseur d'accès doit être entré manuellement dans le fichier `/etc/named.conf` dans la catégorie `forwarders` avec son adresse IP.

Astuce

DNS et pare-feu

Si vous utilisez un pare-feu, vous devez veiller à ce qu'il laisse passer les requêtes DNS.

Astuce

33.5 Le fichier de configuration /etc/squid/squid.conf

Vous devez effectuer tous les réglages du serveur proxy Squid dans le fichier `/etc/squid/squid.conf`. Pour pouvoir démarrer Squid la première fois, aucune modification n'est nécessaire, mais dans un premier temps l'accès est interdit aux clients externes. Le serveur proxy est accessible à `localhost`. C'est le port `3128` qui est utilisé par défaut. Vous trouverez des explications complètes des options et de nombreux exemples dans le fichier `/etc/squid/squid.conf` préinstallé. Presque toutes les lignes sont précédées d'un signe # (les lignes sont mises en commentaire) et les réglages correspondants se trouvent en fin de ligne. Les valeurs indiquées correspondent presque toujours aux valeurs par défaut, si bien que la suppression du signe de commentaire sans modifier le paramètre de l'option n'a, à quelques exceptions près, aucun effet. Il est donc préférable de conserver l'exemple en l'état et de recopier l'option avec le paramètre modifié sur la ligne en-dessous. Vous pouvez ainsi distinguer sans problème les valeurs prédéfinies et les modifications qui y sont apportées.

Astuce

Adapter le ficher de configuration après une mise à jour

Si vous avez effectué une mise à jour à partir d'une version plus ancienne de Squid, il est recommandé d'utiliser le nouveau fichier `/etc/squid/squid.conf` et de ne reprendre que les modifications du fichier précédent. Si vous essayez de continuer à utiliser l'ancien `squid.conf`, vous courez le risque que votre configuration ne fonctionne plus, parce que les options sont parfois modifiées et que de nouvelles sont ajoutées.

Astuce

33.5.1 Quelques options de configuration générales

http_port 3128 C'est le port sur lequel Squid écoute les demandes des clients. La valeur par défaut est `3128`, mais `8080` est également fréquemment utilisé. Il est possible d'indiquer ici plusieurs numéros de port en les séparant par des espaces.

cache_peer nom_hote type port_proxy port_icp
Saisissez ici un serveur proxy de niveau supérieur, par exemple lorsque vous souhaitez utiliser celui de votre fournisseur d'accès. Indiquez dans ⟨*nom_hote*⟩ le nom et l'adresse IP du serveur proxy à utiliser et comme ⟨*type*⟩, `parent`. Indiquez dans ⟨*port_proxy*⟩ le numéro de port du gestionnaire du serveur parent qui doit être utiliser dans le navigateur, en général `8080`. Réglez ⟨*port_icp*⟩ à `7` ou `0` si vous ne connaissez pas le port ICP du parent ou si l'utilisation de celui-ci n'a pas été convenue avec le fournisseur d'accès. Vous devez encore préciser `default` et `no-query` après le numéro de port pour empêcher complètement l'utilisation du protocole ICP. Squid se comporte alors comme un navigateur normal vis-à-vis du serveur proxy du fournisseur d'accès.

cache_mem 8 MB Cette déclaration indique la taille maximale de la mémoire centrale utilisée par Squid pour les caches. La valeur par défaut est `8 Mo`.

cache_dir ufs /var/cache/squid 100 16 256
La déclaration *cache_dir* indique le répertoire dans lequel tous les objets sont stockés sur le disque. Les nombres derrière indiquent l'espace disque maximal à utiliser en "Mo" et le nombre des répertoires dans les premier et deuxième niveaux. Ne modifiez pas le paramètre `ufs`. L'espace disque défini par défaut est de `100 Mo` dans le répertoire `/var/cache/squid`, soit 16 sous-répertoires contenant chacun environ 256 répertoires. Lorsque l'on indique l'espace disque à utiliser, il faut prévoir suffisamment de marge. Des valeurs comprises entre 50 et 80 pour cent du disque disponible sont raisonnables, 80 pour cent étant un maximum. N'augmentez les deux derniers valeurs c'est-à-dire le nombre de répertoires qu'avec la plus grande précaution, dans la mesure où trop de répertoires peuvent également avoir des répercussions sur la performance. Si vous disposez de plusieurs disques sur lesquels répartir le cache, insérez autant de lignes *cache_dir* que nécessaire.

cache_access_log /var/log/squid/access.log
Chemin des fichiers journaux

cache_log /var/log/squid/cache.log Chemin des fichiers journaux

cache_store_log /var/log/squid/store.log
Chemin des fichiers journaux

Ces trois déclarations indiquent les chemins d'accès où Squid consigne ses actions dans des journaux. Si Squid doit être fortement sollicité, il peut être judicieux de répartir le cache et les fichiers journaux sur différents disques.

emulate_httpd_log off Si vous réglez ce paramètre à *on*, vous obtiendrez des fichiers journaux lisibles. Certains programmes n'arrivent toutefois pas à les exploiter.

client_netmask 255.255.255.255 Cette déclaration permet de masquer les adresses IP enregistrées dans les fichiers journaux et ainsi de dissimuler l'identité des clients. Si vous indiquez `255.255.255.0` ici, le dernier chiffre de l'adresse IP est mis à zéro.

ftp_user Squid@ Vous pouvez définir ici le mot de passe que Squid doit utiliser pour une connexion FTP anonyme. Il peut être intelligent d'indiquer ici une adresse électronique valable car certains serveurs FTP en vérifient la validité.

cache_mgr adresse Une adresse électronique à laquelle Squid envoie un message lorsqu'il s'arrête de manière inattendue. L'adresse par défaut est *webmaster*.

logfile_rotate 0 Squid peut effectuer une rotation des fichiers journaux sécurisés si vous lancez la commande `squid -k rotate`. Les fichiers sont à cet effet numérotés et lorsque la valeur spécifiée est atteinte, les fichiers les plus anciens sont écrasés. Cette valeur est par défaut fixée à `0`, car l'archivage et la suppression des fichiers journaux dans SUSE LINUX est effectué par une tâche cron propre configurée dans le fichier `/etc/logrotate/squid`.

append_domain domaine Avec *append_domain*, vous pouvez indiquer quel domaine doit être automatiquement ajouté lorsqu'aucun n'est spécifié. On indique ici la plupart du temps son propre domaine et il suffit alors de saisir *www* dans le navigateur pour accéder à son propre serveur web.

forwarded_for on Si vous réglez ce paramètre à *off*, Squid retire les adresses IP et les noms de machine des clients contenus dans les requêtes HTTP.

negative_ttl 5 minutes; negative_dns_ttl 5 minutes
Vous n'avez normalement pas besoin de modifier ces valeurs. Si toutefois vous disposez d'une liaison commutée, il se peut que l'Internet ne puisse parfois pas être joint. Squid note les demandes qui ont échoué et refuse ensuite de procéder à de nouvelles requêtes même si la connexion Internet a été rétablie. Dans ce cas, vous devez remplacer *minutes* par *seconds* puis, en

cliquant sur *recharger* dans le navigateur, la connexion devrait être rétablie après quelques secondes.

never_direct allow nom_acl Si vous souhaitez empêcher que Squid n'interroge directement l'Internet, utilisez la commande ci-dessus pour forcer l'utilisation d'un autre serveur proxy. Vous devez avoir au préalable saisi celui-ci sous *cache_peer*. Si vous indiquez `all` en tant que ⟨*nom_acl*⟩, vous forcez le transfert de toutes les demandes au *parent*. Cela peut être utile, par exemple, si vous passez par un fournisseur d'accès qui exige que vous utilisiez son serveur proxy, ou si le pare-feu n'autorise aucun accès direct à l'Internet.

33.5.2 Options liées au contrôle d'accès

Squid propose un système détaillé pour gérer l'accès au serveur proxy. L'utilisation d'ACL (listes de contrôle d'accès) permet de le configurer facilement et complètement. Il s'agit de listes de règles traitées en séquence. Vous devez commencer par définir des ACL pour pouvoir les utiliser. Quelques ACL usuelles telles que *all* et *localhost* sont déjà disponibles. La définition d'une ACL en soi n'a cependant aucun effet. Ce n'est qu'une fois réellement installée en relation avec *http_access* qu'une règle définie est appliquée.

acl nom_acl type donnees Pour définir une ACL, il faut au moins trois informations. Vous pouvez choisir son nom *nom_acl* librement. Pour le *type*, vous pouvez choisir parmi un large éventail de possibilités que vous pouvez consulter dans la section *ACCESS CONTROLS* du fichier `/etc/squid/squid.conf`. Les données, *donnees*dépendent du type de l'ACL et peuvent également être lues depuis un fichier, il peut par exemple s'agir de noms d'ordinateur, d'adresses IP ou d'URL. En voici quelques exemples simples :

```
acl mes_surfeurs srcdomain .mon_domaine.com
acl professeur src 192.168.1.0/255.255.255.0
acl etudiants src 192.168.7.0-192.168.9.0/255.255.255.0
acl midi time MTWHF 12:00-15:00
```

http_access allow nom_acl Utilisez *http_access* pour définir qui est autorisé à utiliser le serveur proxy et à quoi il peut accéder sur l'Internet. Pour ce faire, saisissez des ACL qui interdiront l'accès avec *deny* ou l'autoriseront avec *allow* ; *localhost* et *all* ont déjà été définis plus haut. Vous pouvez créer ici une liste comprenant plusieurs déclarations *http_access* ; ainsi, selon ce qui se produit en premier, l'accès à l'URL demandée sera ou non autorisé. La dernière déclaration doit toujours être *http_access deny all*. Dans l'exemple

suivant, *localhost*, c'est-à-dire l'ordinateur local a un accès libre à tout, tandis que tout est complètement bloqué pour tous les autres :

```
http_access allow localhost
http_access deny all
```

Encore un exemple dans lequel sont utilisées les ACL définies précédemment : le groupe `professeurs` a tout le temps accès à l'Internet, tandis que le groupe `etudiants` n'y a accès que du lundi au vendredi et seulement pendant la pause de midi :

```
http_access deny localhost
http_access allow professeurs
http_access allow etudiants midi time
http_access deny all
```

Pour des raisons de clarté, n'insérez dans la liste vos propres déclarations *http_access* qu'à l'endroit prévu à cet effet dans le fichier `/etc/squid/squid.conf`. Cela signifie entre le texte

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

et la déclaration finale

```
http_access deny all
```

redirect_program /usr/bin/squidGuard
Vous pouvez utiliser cette option pour indiquer un redirecteur, comme squidGuard, qui est en mesure de bloquer l'accès aux URL indésirables. Il est donc possible de gérer individuellement l'accès à l'Internet de différents groupes d'utilisateurs à l'aide de l'authentification sur le serveur proxy et des ACL adaptées. squidGuard est un paquetage indépendant que l'on peut installer et configurer.

auth_param basic program /usr/sbin/pam_auth
Si les utilisateurs doivent s'authentifier auprès du serveur proxy, vous pouvez indiquer ici un programme responsable de l'authentification, comme pam_auth. Lorsque pam_auth est utilisé, une fenêtre d'authentification s'ouvre lors de sa première tentative de connexion, dans laquelle l'utilisateur doit saisir son nom d'utilisateur et son mot de passe. Vous avez besoin, en outre, d'une ACL supplémentaire pour n'autoriser que les clients disposant d'un login valable à naviguer sur l'Internet :

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Vous pouvez remplacer le mot-clé *REQUIRED* après *proxy_auth* par une liste de noms d'utilisateurs autorisés ou par le chemin d'accès à cette liste.

ident_lookup_access allow nom_acl Cette option permet qu'une demande d'identification soit adressée à tous les clients définis à l'aide d'ACL pour vérifier l'identité de chaque utilisateur. Si vous attribuez à *nom_acl* la valeur *all*, cela s'applique de manière générale à tous les clients. De plus, un démon ident doit fonctionner sur tous les clients. Pour cela, installez sous Linux le paquetage pidentd. Sous `Windows`, il existe un logiciel gratuit pouvant être téléchargé sur l'Internet. Pour que seuls soient autorisés les clients dont la recherche d'identité a réussi, il faut ici définir une ACL correspondante :

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

Vous pouvez ici aussi remplacer le terme *REQUIRED* par une liste de noms d'utilisateurs autorisés. L'utilisation d'*ident* peut considérablement ralentir l'accès dans la mesure où la recherche d'identité est répétée en entier à chaque demande.

33.6 Configuration d'un serveur proxy transparent

Normalement, le navigateur web envoie les demandes à un port donné du serveur proxy et le serveur proxy fournit les objets demandés, qu'ils soient ou non en cache. Dans un vrai réseau, différentes situations peuvent se présenter :

- Pour des raisons de sécurité, il vaut mieux que tous les clients utilisent un serveur proxy pour naviguer sur l'Internet.
- Il est indispensable que tous les clients utilisent un serveur proxy qu'ils en soient ou non informés.

- Si le serveur proxy d'un réseau déménage, les clients existants doivent quand même conserver leur ancienne configuration.

Vous pouvez utiliser un serveur proxy transparent dans chacun des cas mentionnés ci-dessus. Le principe est très simple : le serveur proxy accepte les demandes du navigateur web et les traite de manière à ce que le navigateur web obtienne les pages demandées sans savoir d'où elles proviennent. Le processus complet s'exécute de manière transparente, d'où son nom.

33.6.1 Configuration du noyau

Vous devez commencer par vous assurer que le noyau du serveur proxy prend en charge un serveur proxy transparent. Le noyau livré avec SUSE LINUX est déjà configuré de façon appropriée. Dans le cas contraire, ajoutez ces options au noyau et recompilez-le. Vous trouverez des informations précises à ce sujet dans le chapitre 9 page 207.

33.6.2 Options de configuration de /etc/squid/squid.conf

Vous devez activer les options suivantes dans le fichier `/etc/squid/squid.conf` pour définir un serveur proxy transparent :

- `httpd_accel_host` virtual
- `httpd_accel_port` 80
  Port, sur lequel se trouve le véritable serveur HTTP.
- `httpd_accel_with_proxy` on
- `httpd_accel_uses_host_header` on

33.6.3 Configuration du pare-feu avec SuSEfirewall2

Toutes les demandes entrantes qui passent au travers du pare-feu doivent être redirigées vers le port de Squid à l'aide d'une règle de redirection de port. Utilisez pour ce faire l'outil SuSEfirewall2 fourni. Il se configure à l'emplacement `/etc/sysconfig/SuSEfirewall2`. Le fichier de configuration se compose de déclarations bien documentées. Même si vous souhaitez seulement installer un serveur proxy transparent, il vous faut configurer quelques options de pare-feu :

- L'interface est du côté de l'Internet : `FW_DEV_EXT`="eth1"
- L'interface est du côté du réseau interne : `FW_DEV_INT`="eth0"

Définissez sur le pare-feu les ports et services (voir `/etc/services`) qui sont accessibles depuis des réseaux (externes) non dignes de confiance comme Internet. Dans cette exemple, seuls les services web sont offerts à l'extérieur :

```
FW_SERVICES_EXT_TCP="www"
```

Définissez sur le pare-feu les ports et services (voir `/etc/services`) qui sont accessibles depuis des réseaux (internes) dignes de confiance, par TCP et UDP :

```
FW_SERVICES_INT_TCP="domain www 3128"
FW_SERVICES_INT_UDP="domain"
```

Cela permet d'accéder aux services web et à Squid (dont le port par défaut est `3128`). Le service "domain" signifie DNS (Domain Name Service). Il s'agit d'un service utilisé fréquemment. Sinon, vous devez simplement supprimer la déclaration ci-dessus et définir l'option suivante à `no` :

```
FW_SERVICE_DNS="yes"
```

L'option la plus importante est le nombre `15` :

Example 33.1: *L'option 15 de la configuration du pare-feu*

```
#
# 15.)
# Quel accès aux différents services doit être redirigé vers un
# port local de l'ordinateur pare-feu ?
#
# Cette option permet d'obliger tous les utilisateurs internes à
# utiliser le serveur proxy pour naviguer ou de transférer
# tout le trafic web entrant à un serveur web sécurisé.
#
# Choix : n'insérer aucune nouvelle déclaration ou utiliser la syntaxe
# de règle de redirection suivante séparée par des espaces.
# Une règle de redirection se compose de : 1) IP/réseau source,
# 2) IP/ réseau cible, 3) port cible précédent et 4) port local
# vers lequel le trafic doit être redirigé, séparés par des
# virgules, par exemple :
# "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
#
```

La syntaxe à respecter est indiquée dans le commentaire ci-dessus. D'abord, indiquez les adresses IP et le masque réseau des réseaux internes qui accèdent au pare-feu du serveur proxy. Ensuite, configurez les adresses IP et le masque réseau auxquels sont envoyées les demandes des clients. Pour les navigateurs web, on choisit les réseaux `0/0`. Il s'agit d'un joker qui signifie "dans toutes les directions." Vient ensuite le port d'origine auquel ces demandes ont été envoyées et enfin le port vers lequel les demandes sont redirigées. Comme Squid prend en charge d'autres protocoles que le seul HTTP, redirigez les demandes provenant d'autres ports au serveur proxy, comme par exemple FTP (port 21), HTTPS ou SSL (port 443). Dans cet exemple, les services web (port `80`) sont redirigés vers le port du serveur proxy (port `3128`. Si plusieurs réseaux ou services doivent être ajoutés, ils doivent être séparés par un espace dans la ligne correspondante.

```
FW_REDIRECT_TCP="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"
FW_REDIRECT_UDP="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"
```

Pour démarrer le pare-feu et la nouvelle configuration, vous devez modifier une ligne du fichier `/etc/sysconfig/SuSEfirewall2`. Le paramètre `START_FW` doit être défini à "yes" :

Démarrez Squid comme expliqué dans la section 33.4 page 610. Utilisez les fichiers journaux dans `/var/log/squid/access.log` pour vérifier que tout fonctionne correctement.

Pour vérifier que tous les ports sont correctement configurés, exécutez une analyse des ports de l'ordinateur à partir de n'importe quel ordinateur extérieur au réseau. Seul le port du service web (port 80) doit être ouvert. Pour analyser les ports avec nmap, la syntaxe de la commande est `nmap -O adresse_IP`.

33.7 cachemgr.cgi

Le gestionnaire de cache (cachemgr.cgi) est un programme CGI utilisé pour générer des statistiques sur l'espace mémoire utilisé par un processus Squid en cours. Il constitue aussi un moyen plus pratique pour gérer le cache et afficher des statistiques sans avoir à tenir un journal de l'activité du serveur.

33.7.1 Mise en place

Vous avez tout d'abord besoin d'un serveur web en état de marche sur le système. En tant que `root`, saisissez la commande suivante pour savoir si Apache fonctionne déjà : `rcapache status`. Si un message comme celui-ci s'affiche :

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

Dans le cas contraire, vous devez saisir la commande suivante : `rcapache start`. Cela vous permet de démarrer Apache avec les paramètres par défaut de SUSE LINUX. Enfin, il faut copier le fichier `cachemgr.cgi` du répertoire `/usr/share/doc/packages/squid/scripts/` dans le répertoire `/srv/www/cgi-bin` d'Apache.

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi /srv/www/cgi-bin/
```

33.7.2 Les ACL du gestionnaire de cache dans /etc/squid/squid.conf

Vous disposez de quelques paramètres par défaut pour le gestionnaire de cache dans le fichier original. La première ACL est la plus importante car le gestionnaire de cache essaie de communiquer avec Squid en utilisant le protocole cache_object.

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Les règles suivantes doivent également être contenues :

```
http_access allow manager localhost
http_access deny manager
```

Les règles suivantes précisent que le serveur web et Squid s'exécutent sur le même ordinateur. Si la communication entre le gestionnaire de cache et Squid se passe au niveau du serveur web sur un autre ordinateur, ajoutez une ACL supplémentaire comme dans l'exemple 33.2 de la présente page.

Example 33.2: *Règles d'accès*

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # adresse du serveur web
```

Ajoutez ensuite les règles de l'exemple 33.3 page ci-contre.

Example 33.3: *Règles d'accès*

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Il est également possible de configurer un mot de passe pour le gestionnaire s'il faut accéder à des options comme par exemple la fermeture du cache à distance ou l'affichage d'informations étendues sur le cache. Vous devez alors configurer le paramètre `cachemgr_passwd` et la liste des options qui s'affichent avec un mot de passe du gestionnaire. Cette liste apparaît en tant que partie des commentaires dans `/etc/squid/squid.conf`.

Redémarrez Squid à chaque fois que vous avez modifié le fichier de configuration. Pour ce faire, le plus simple est d'utiliser la commande `rcsquid reload`.

33.7.3 Affichage des statistiques

Rendez-vous sur la page web correspondante—`http://webserver.example.org/cgi-bin/cachemgr.cgi`. Cliquez sur 'Continuer' pour afficher les différentes statistiques. Vous trouverez des informations supplémentaires (en anglais) au sujet des différents éléments fournis par le gestionnaire de cache dans la FAQ de Squid : `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html`.

33.8 squidGuard

Ce chapitre ne présente que la configuration de squidGuard et donne quelques conseils relatifs à son utilisation. L'objectif n'est pas ici d'en donner une explication complète. Vous trouverez des informations plus détaillées à ce sujet dans les pages web de squidGuard : `http://www.squidguard.org`.

squidGuard est un filtre libre (sous GPL), flexible et rapide, un redirecteur et un module externe pour les contrôles d'accès de Squid. Il permet de définir un grand nombre de règles d'accès à un cache Squid avec des limitations distinctes en fonction des différents groupes d'utilisateurs. squidGuard utilise l'interface standard de Squid pour la redirection.

Vous pouvez utiliser squidGuard, entre autres, pour :

- Limiter l'accès à l'Internet de certains utilisateurs à des serveurs web et/ou des URL acceptés/connus.
- Refuser l'accès à certains serveurs web et/ou URL à certains utilisateurs.
- Refuser l'accès aux URL qui contiennent des expressions ou des mots particuliers à certains utilisateurs.
- Rediriger les URL bloquées vers une page d'informations CGI "intelligente".
- Rediriger les utilisateurs non enregistrés vers un formulaire d'enregistrement.
- Remplacer les bannières par un GIF vide.
- Utiliser différentes règles d'accès en fonction de l'heure, du jour de la semaine, de la date, etc.
- Utiliser différentes règles pour les différents groupes d'utilisateurs.

squidGuard et Squid ne peuvent pas servir à :

- Filtrer, censurer ou modifier le texte à l'intérieur de documents.
- Filtrer, censurer ou modifier le langage de script intégré dans du HTML, tel que JavaScript ou VBscript.

Installez `squidGuard`. Modifiez le fichier de configuration `/etc/squidguard.conf`. Vous disposez de nombreux autres exemples de configuration à l'adresse `http://www.squidguard.org/config/`. Vous pourrez apprendre plus tard à effectuer des paramétrages plus compliqués.

L'étape suivante consiste à créer une page factice "Accès refusé" ou une page CGI plus ou moins complexe pour rediriger Squid lorsque le client demande une page web interdite. Nous vous recommandons fortement d'utiliser Apache.

À présent, configurez Squid pour qu'il utilise squidGuard. Utilisez pour ce faire la déclaration suivante dans le fichier `/etc/squid/squid.conf` :

```
redirect_program /usr/bin/squidGuard
```

Une autre option appelée `redirect_children` permet de configurer le nombre des différents processus "redirect" exécutés par l'ordinateur, c'est-à-dire des processus de redirection (dans ce cas, squidGuard). squidGuard est suffisamment rapide pour traiter un grand nombre de demandes : sur un Pentium 500 MHz avec 5 900 domaines, 7 880 URL (soit 13 780 au total), il peut traiter 100 000 demandes en 10 secondes. Il est donc préférable de ne pas définir plus de 4 processus car l'allocation de ces processus consomme trop de mémoire.

```
redirect_children 4
```

Enfin, faites lire à Squid le nouveau fichier de configuration : `rcsquid reload`. À présent, testez vos réglages dans un navigateur.

33.9 Génération de rapports de cache avec Calamaris

Calamaris est un script Perl utilisé pour générer des rapports d'activité du cache au format ASCII ou HTML. Il utilise pour ce faire les journaux d'accès de Squid. Voici l'adresse de la page web de Calamaris `http://Calamaris.Cord.de/`. Ce programme est assez simple à utiliser.

Connectez-vous en tant qu'utilisateur `root` et lancez la commande suivante : `cat access.log.files | calamaris ⟨options⟩ > fichier_rapport`. Lorsque vous utilisez plusieurs fichiers journaux, il est important de respecter l'ordre chronologique, c'est-à-dire que les fichiers les plus anciens viennent en premier. Voici les différentes options disponibles :

-a tous les rapports disponibles

-w rapport HTML

-l message ou logo dans l'en-tête du rapport

Pour plus d'informations sur les différentes options, consultez la page de manuel de Calamaris : `man calamaris`.

Un exemple typique est

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \
> /usr/local/httpd/htdocs/Squid/squidreport.html
```

Cela place le rapport dans le répertoire du serveur web. Il faut utiliser Apache pour voir les rapports.

SARG (Squid Analysis Report Generator) est un autre outil puissant utilisé pour générer des rapports de cache. Pour plus d'informations à son sujet, consultez la page : `http://web.onda.com.br/orso/`.

33.10 Pour plus d'informations sur Squid

Consultez le site Internet de Squid à l'adresse `http://www.squid-cache.org/`. Vous y trouverez le guide de l'utilisateur de Squid ("Squid User Guide") et une FAQ complète au sujet de Squid.

Le paquetage howtoen propose un mini-descriptif (howto) des serveurs proxy transparents que vous trouverez sous /usr/share/doc/howto/en/mini/TransparentProxy.gz après l'installation. Enfin, vous trouverez des listes de diffusion concernant Squid à l'adresse squid-users@squid-cache.org. L'archive correspondante se trouve à l'adresse http://www.squid-cache.org/mail-archive/squid-users/.

Quatrième partie

Administration

Sécurité sous Linux

La mascarade et les pare-feux permettent de contrôler le trafic et l'échange des données. L'interpréteur de commandes sécurisé (Secure Shell, SSH) permet à l'utilisateur de se connecter à une machine distante par une liaison chiffrée. Le chiffrement des fichiers ou de partitions entières sécurise vos données lorsque des tiers ont accès à votre système. Outre ces instructions purement techniques, vous trouverez, en conclusion, une section traitant de différents aspects de la sécurité dans les réseaux Linux.

34.1 Masquage et pare-feu

Lorsque Linux est utilisé dans un environnement réseau, vous pouvez utiliser les fonctionnalités du noyau pour manipuler les paquets réseau afin de maintenir une séparation entre les secteurs externe et interne du réseau. L'infrastructure Netfilter offre les moyens d'établir un pare-feu efficace maintenant la séparation entre des réseaux différents. Iptables — une structure de table générique permettant de définir des ensembles de règles — permet un contrôle précis des paquets autorisés à transiter par l'interface réseau. Vous pouvez mettre en place un tel filtre de paquets de façon assez simple avec l'aide de SuSEfirewall2 et du module correspondant de YaST.

34.1.1 Filtrage de paquets avec iptables

Les composants netfilter et iptables sont chargés de filtrer et de manipuler les paquets réseau, ainsi que de traduire les adresses réseau (NAT, Network Address Translation). Les critères de filtrage ainsi que toute action leur étant associée sont enregistrés dans des chaînes qui doivent être vérifiées l'une après l'autre par tout paquet réseau entrant. Les chaînes de règles sont enregistrées dans des tables. La commande `iptables` a permet de modifier ces tables et ces ensembles de règles.

Linux dispose de trois tables pour les différentes fonctions d'un filtre de paquets :

filter La plupart des règles se trouvent dans cette table puisque le *filtrage de paquets* proprement dit y est défini. Les règles concernant l'admission (`ACCEPT`) et l'abandon (`DROP`) des paquets y figurent.

nat La modification des adresses sources et cibles des paquets est définie ici. Le *masquage* dont vous vous servez pour la connexion d'un petit réseau privé à l'Internet est un cas particulier de NAT.

mangle Les valeurs contenues dans l'en-tête IP peuvent être manipulées à l'aide des règles fixées ici (le *type de service*).

Dans les tables citées, il y a plusieurs chaînes prédéfinies par lesquelles les paquets doivent passer :

PREROUTING Cette chaîne concerne les paquets qui viennent d'arriver au système.

INPUT Cette chaîne concerne les paquets qui sont destinés à des processus propres au système.

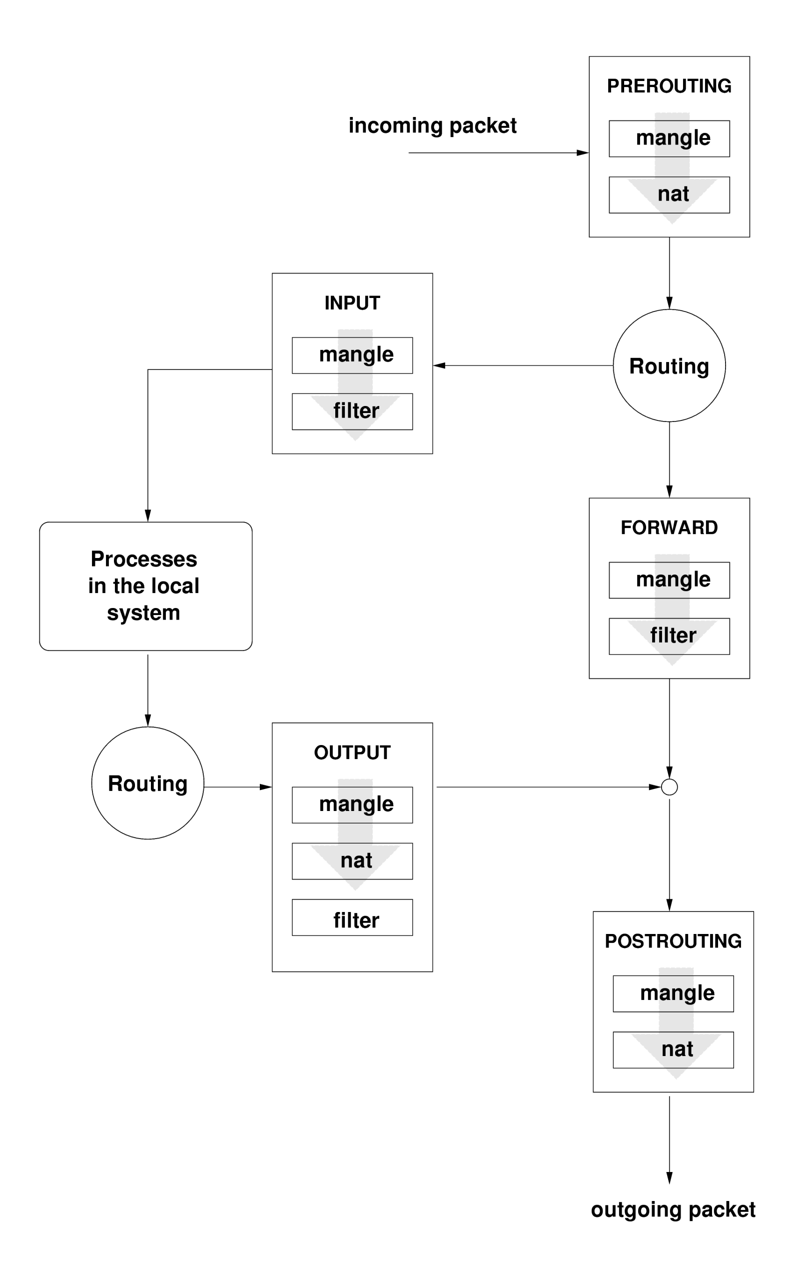


FIG. 34.1: *iptables~: chemins pouvant être suivis par un paquet*

FORWARD Cette chaîne concerne les paquets qui sont simplement routés à travers le système.

OUTPUT Cette chaîne concerne les paquets qui ont été générés dans le système lui-même.

POSTROUTING Cette chaîne concerne tous les paquets qui quittent le système.

La figure 34.1 page précédente illustre le cheminement possible d'un paquet réseau à travers le système. Pour la clarté de l'exposé, les tables sont groupées par chaînes, bien que dans la réalité les chaînes se trouvent à l'intérieur des tables.

Dans le cas le plus simple, un paquet qui est destiné au système lui-même arrive sur l'interface `eth0` du système. Ce paquet est d'abord dirigé dans la chaîne `PREROUTING` de la table `mangle`, puis dans la chaîne `PREROUTING` de la table `nat`. L'étape de routage suivante permet d'établir que le paquet est destiné à un processus dans le système lui-même. Après être passé par la chaîne `INPUT` dans les deux tables `mangle` et `filter`, le paquet arrive à son lieu de destination, en supposant que les règles de filtrage dans la table ne l'en empêchent pas.

34.1.2 Principes de base du masquage

Le masquage est le cas particulier sous Linux de NAT (Network Address Translation), la traduction des adresses réseau. Il est mis en œuvre quand un petit réseau local ayant ses adresses IP du domaine privé (voir la section 22.1.2 page 420) est connecté à l'Internet avec ses adresses IP officielles. Pour que les ordinateurs du réseau local puissent établir des connexions à l'Internet, une correspondance entre les adresses privées et les adresses officielles s'impose. Ce processus a lieu sur le routeur, qui sert de passerelle entre le réseau local et l'Internet. Le principe sous-jacent est simple : le routeur possède plusieurs interfaces réseau, généralement une carte réseau et une interface séparée d'accès à l'Internet. Celle-ci raccorde le routeur à l'extérieur, tandis qu'une ou plusieurs autres le raccordent aux ordinateurs du réseau local. Les ordinateurs du réseau local étant connectés à la carte réseau du routeur (par exemple `eth0`), ils peuvent envoyer à leur passerelle par défaut ou au routeur tous les paquets non destinés au réseau local.

Comme expliqué plus haut, si un des ordinateurs de votre réseau envoie un paquet destiné à l'Internet, ce paquet arrive sur le routeur par défaut. Toutefois, celui-ci doit préalablement être configuré de manière à transmettre aussi ce type de paquets. Pour des raisons de sécurité, SUSE LINUX ne permet pas, par défaut, un tel fonctionnement. Pour activer cette fonctionnalité, modifiez la variable `IP_FORWARD` dans le fichier `/etc/sysconfig/sysctl` pour lui attribuer la valeur `IP_FORWARD=yes`.

Important

Utiliser le bon masque réseau

Lorsque vous configurez votre réseau, veillez toujours à la concordance entre les adresses de diffusion et les masques réseau. Autrement, votre réseau ne fonctionnera pas correctement, puisque les paquets réseau ne pourront pas être routés.

Important

L'ordinateur cible de la connexion ne connaît que votre routeur, et non l'ordinateur expéditeur de votre réseau interne proprement dit. Celui-ci se cache derrière votre routeur. C'est de là que vient le terme de masquage. Du fait de la traduction d'adresses, l'adresse cible pour les paquets reçus est à nouveau notre routeur. Ce dernier doit reconnaître les paquets et réécrire l'adresse cible de manière à ce qu'ils arrivent sur l'ordinateur qui convient dans le réseau local.

Comme le chemin parcouru par les paquets de l'extérieur vers l'intérieur dépend du tableau de masquage, il n'est pas possible d'ouvrir une connexion de l'extérieur vers l'intérieur. Il n'y aurait pour cette connexion aucun élément dans le tableau. Une connexion établie possède ainsi un état particulier dans ce tableau, de manière à ce que cet élément de tableau ne puisse être utilisé par une deuxième connexion.

En conséquence, on rencontre à présent des problèmes avec certaines applications, ICQ, CU-SeeMe, IRC (DCC, CTCP) et FTP (en mode PORT). Netscape, le programme FTP standard et beaucoup d'autres applications utilisent le mode PASV qui, en ce qui concerne le filtrage des paquets et le masquage, rencontre beaucoup moins de problèmes.

34.1.3 Principes de base du pare-feu

Le terme *pare-feu* est probablement le terme le plus utilisé pour décrire un mécanisme qui fournit et gère une connexion entre deux réseaux mais en contrôlant le trafic autant que possible. Au sens strict du terme, le mécanisme décrit dans cette section serait plus correctement désigné par l'expression *filtre de paquets*. Un filtre de paquets régule le passage des données au moyen de critères tels que le protocole, le port et l'adresse IP. De cette manière, vous pouvez bloquer des paquets qui, en raison de leur adressage, ne devraient pas s'infiltrer dans votre réseau. Si, par exemple, vous souhaitez autoriser les accès à votre serveur web, vous devez explicitement ouvrir le port correspondant. Toutefois, un filtre de paquets

ne contrôle pas le contenu de paquets adressés correctement, comme ceux ayant votre serveur web pour cible. Ainsi, si un paquet est envoyé dans le but d'attaquer l'un des programmes CGI de votre serveur web, votre filtre de paquets le laissera passer.

Une structure plus efficace—mais aussi plus complexe—consiste à combiner plusieurs types de systèmes, par exemple, un filtre de paquets interagissant avec des passerelles applicatives ou des serveurs mandataires supplémentaires. Dans ce cas, le filtre de paquets rejette tous les paquets destinés à des ports non ouverts. Seuls les paquets destinés à une passerelle applicative doivent pouvoir être autorisés à passer. Ce serveur mandataire fonctionne alors comme s'il s'agissait du véritable interlocuteur du serveur qui établit une connexion avec nous. En ce sens, un tel serveur mandataire peut être considéré comme une machine de masquage au niveau du protocole de chaque application. Un exemple de ce type de serveur mandataire est Squid, un serveur mandataire HTTP. Pour utiliser Squid, vous devez configurer votre navigateur de manière à communiquer à travers le proxy. La mémoire cache du serveur mandataire répond à toute demande de page HTML, et si une page n'y est pas enregistrée, c'est le serveur mandataire qui récupère la page depuis l'Internet. Un autre exemple serait SuSE proxy-suite (paquetage `proxy-suite`) qui propose un serveur mandataire pour le protocole FTP.

Nous souhaitons à présent nous concentrer sur le paquetage "filtre de paquets" de SUSE LINUX. Pour obtenir plus d'informations ainsi que d'autres liens à propos des pare-feu, consultez le document Firewall-HOWTO (en anglais) contenu dans le paquetage `howto`. Pour le lire, utilisez la commande `less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz` si ce paquetage est installé.

34.1.4 SuSEfirewall2

SuSEfirewall2 est un script qui convertit les variables configurées dans `/etc/sysconfig/SuSEfirewall2` en un ensemble de règles iptables. SuSEfirewall2 définit trois zones de sécurité cependant, dans l'exemple de configuration suivant, on ne prendra en considération que les deux premières zone :

Zone externe L'ordinateur doit être protégé du réseau externe, puisque ce dernier n'est pas sous contrôle à proprement parler. Il est généralement question ici de l'Internet, mais il peut tout aussi bien s'agir d'autres réseaux non protégés (un réseau étendu).

Zone interne Ici, il est question du réseau privé, généralement un réseau local. Si l'on utilise dans ce réseau des adresses IP du domaine privé (voir la section 22.1.2 page 420), la mise en œuvre de la traduction d'adresses réseau (NAT) s'impose pour pouvoir accéder du le réseau interne vers l'extérieur.

Zone démilitarisée (DMZ) Les ordinateurs qui se trouvent dans cette zone sont accessibles du réseau externe comme du réseau interne mais n'ont aucun accès au réseau interne. Ce type de configuration est une protection additionnelle du réseau interne vis-à-vis du réseau externe, puisque les machines de la zone démilitarisée sont isolées du réseau interne.

Tout trafic réseau qui n'a pas fait l'objet d'une autorisation explicite dans le jeu de règles de filtrage est interrompu par iptables. Par conséquent, chaque interface ayant un trafic entrant doit être affectée à une des trois zones. Pour chacune de ces zones, il faut définir les services ou protocoles autorisés. L'ensemble de règles ne contrôle toutefois que les paquets provenant d'hôtes distants. Les paquets générés localement ne sont pas filtrés par le pare-feu.

La configuration se fait soit avec YaST (voir la section Configuration avec YaST de la présente page), soit manuellement dans le fichier `/etc/sysconfig/SuSEfirewall2` qui contient des commentaires détaillés en anglais. Vous trouverez de plus quelques exemples de scénarios dans `/usr/share/doc/packages/SuSEfirewall2/EXAMPLES`.

Configuration avec YaST

Important

Configuration automatique du pare-feu

Après l'installation, YaST démarre automatiquement un pare-feu sur toutes vos interfaces configurées. Si un serveur est configuré et activé sur votre système, YaST modifie la configuration du pare-feu générée automatiquement au travers des options 'Ouvrir le pare-feu sur les ports sélectionnés' ou 'Ouvrir port sur pare-feu' du module de configuration du serveur. Certaines boites de dialogue de module serveur proposent un bouton 'Détails du pare-feu' permettant d'activer d'autres services ou ports. Le module de YaST pour la configuration du pare-feu sert à activer ou désactiver le pare-feu ou à le reconfigurer indépendamment.

Important

Utilisez le centre de contrôle de YaST pour accéder à la configuration en mode graphique. Choisissez dans la catégorie 'Sécurité et utilisateurs' l'option 'Pare-feu'. La configuration se divise en sept sous-sections auxquelles on peut accéder directement dans la partie gauche de l'arborescence à l'écran.

Démarrage Définissez le comportement au démarrage dans ce dialogue. Dans l'installation par défaut, SuSEfirewall2 fonctionne déjà sur un système nouvellement installé. Vous pouvez également démarrer et arrêter le pare-feu ici. Si vous souhaitez tester les paramètres actuels de votre pare-feu, utilisez le bouton 'Enregistrer les paramètres et redémarrer le pare-feu maintenant'.

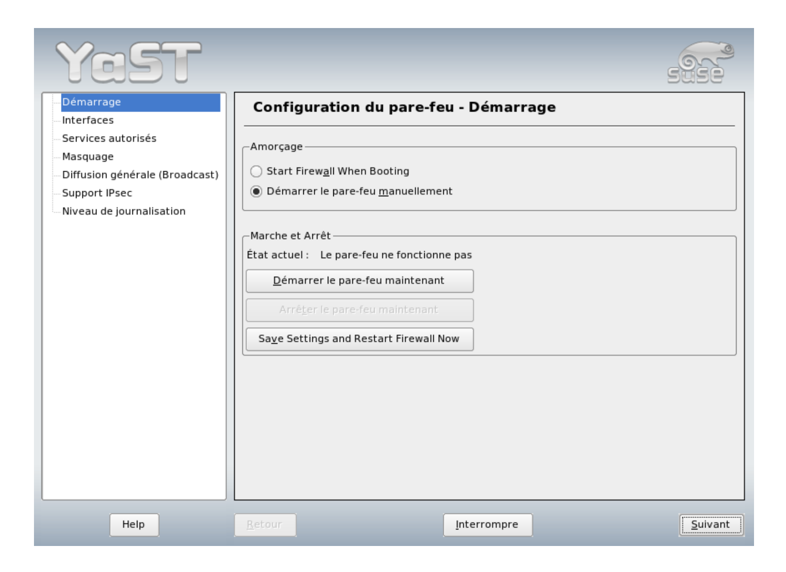


FIG. 34.2: *La configuraton YaST du pare-feu*

Interfaces Toutes les interfaces réseau connues sont répertoriées ici. Pour supprimer une interface d'une zone, sélectionnez l'interface, cliquez sur 'Changer' et choisissez '____pas_de_zone____'. Pour ajouter une interface dans une zone, sélectionnez l'interface, cliquez sur 'Changer' et choisissez une des zones disponibles. Vous pouvez également créer une interface spéciale avec vos propres paramètres en utilisant 'Personnalisé'.

Services autorisés Vous nécessitez cette option pour offrir des services de votre système à une zone protégée. Par défaut, seule la zone externe est protégée. Dans ce cas, vous devez autoriser explicitement les services qui doivent

être vus par des hôtes externes. Après avoit sélectionné la zone concernée, activez le service correspondant dans 'Services autorisés pour la zone sélectionnée'.

Masquage Le masquage vous permet de cacher votre réseau interne des réseaux externes comme Internet. Il permet aussi au réseau interne d'accéder au réseau externe de façon transparente. Les requêtes du réseau externe vers le réseau interne sont bloquées alors que les requêtes du réseau interne vers le réseau externe semblent être faites par le serveur de masquage lorsqu'elles sont vues à l'extérieur.

Si des services spéciaux d'une machine interne doivent être disponibles pour le réseau externe, vous pouvez ajouter des règles spéciales de redirection pour les services correspondants.

Diffusion générale (Broadcast) Dans ce dialogue, les ports UDP qui permettent les diffusions générales sont configurés. Les numéros ou services de port nécessaires doivent être ajoutés à la zone correspondante en les séparant par un espace. Voyez également le fichier `/etc/services`.

La journalisation des diffusions générales non autorisées peut être activée ici. Cela peut être problématique car les hôtes Windows utilisent les diffusions générales pour se connaître les uns les autres et génèrent donc de nombreux paquets non autorisés.

Support IPsec Dans ce dialogue, vous pouvez définir si le service IPsec sera autorisée depuis le réseau externe. La configuration des paquets qui sont de confiance doit être faite sous 'Détails'.

Niveau de journalisation Il existe deux règles de journalisation paquets autorisés ou non autorisés. Les paquets autorisés sont ACCEPTÉS, les paquets non autorisés sont ABANDONNÉS ou REJETÉS. Pour ces deux règles, vous pouvez sélectionner parmi 'Tout journaliser', 'Journaliser ce qui est critique' ou 'Ne rien journaliser'.

Lorsque vous avez terminé la configuration du pare-feu, quittez ce formulaire en cliquant sur 'Suivant'. Vous obtenez alors un résumé par zone de la configuration du pare-feu où vous pouvez encore vérifier tous les paramètres. Tous les services ports et protocoles qui ont été autorisés sont répertoriés dans le résumé. Si vous voulez retourner en arrière dans la configuration, utilisez 'Retour', sinon cliquez sur 'Accepter' afin d'enregistrer votre configuration.

Configuration manuelle

Voyons à présent étape par étape une configuration réussie. Nous préciserons, pour chaque point, s'il s'agit de masquage ou de pare-feu. Dans le fichier de

configuration, il est aussi question d'une zone démilitarisée (DMZ, en anglais demilitarized zone), que nous n'étudierons pas en détail pour l'instant. En effet, on n'utilise de zone démilitarisée que dans le cadre d'une infrastructure réseau plus complexe, qu'on trouve dans des organisations de grande envergure (réseaux d'entreprise), et qui demandent une configuration extensive et des connaissances détaillées sur le sujet.

Activez d'abord SuSEfirewall2 pour votre niveau d'exécution (probablement 3 ou 5) avec le module de YaST Éditeur de niveaux d'exécution. Il crée les liens symboliques pour les scripts SuSEfirewall2_* dans les répertoires `/etc/init.d/rc?.d/`.

`FW_DEV_EXT` (pare-feu, masquage) Il s'agit de l'interface connectée à l'Internet. Pour une connexion par modem, saisissez `ppp0`, et à `ippp0` pour une connexion RNIS. Les connexions DSL utilisent `dsl0`. Indiquez `auto` pour utiliser l'interface correspondant à la route par défaut.

`FW_DEV_INT` (pare-feu, masquage) Indiquez ici l'interface qui pointe sur le réseau "privé" interne (`eth0`). S'il n'existe aucun réseau interne, contentez-vous de laisser ce champ vide.

`FW_ROUTE` (pare-feu, masquage) Si vous avez besoin du masquage, vous devez impérativement indiquer `yes` ici. Vos machines internes ne sont pas visibles de l'extérieur, car elles possèdent des adresses réseau privées (`192.168.x.x`) qui ne sont pas routées sur l'Internet.

Dans le cas d'un pare-feu sans masquage, ne choisissez ici `yes` que si vous souhaitez autoriser l'accès à votre réseau interne. Vous devez pour cela avoir affecté des adresses IP officielles aux machines internes. Vous ne devriez normalement *pas* autoriser l'accès de l'extérieur à vos machines internes !

`FW_MASQUERADE` (masquage) Si vous avez besoin du masquage, vous devez indiquer `yes` ici. Ceci offre une connexion à Internet virtuellement directe aux hôtes internes. Notez qu'il est plus sûr d'avoir un serveur mandataire entre les ordinateurs du réseau interne et l'Internet. Le masquage n'est pas nécessaire pour les services qu'un serveur proxy fournit.

`FW_MASQ_NETS` (masquage) Indiquez ici les ordinateurs ou les réseaux pour lesquels il faut faire du masquage. Séparez chaque saisie par un espace. Par exemple :

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

FW_PROTECT_FROM_INT (pare-feu) Saisissez ici yes si vous souhaitez aussi protéger l'ordinateur utilisé comme pare-feu contre les tentatives d'attaque en provenance du réseau interne. Vous devez alors autoriser explicitement les services disponibles pour le réseau interne. Voir également FW_-SERVICES_INT_TCP et FW_SERVICES_INT_UDP.

FW_SERVICES_EXT_TCP (pare-feu) Indiquez ici les ports TCP auxquels on doit pouvoir accéder. Pour un simple ordinateur domestique qui n'a pas à proposer de services, vous n'avez la plupart du temps rien à indiquer.

FW_SERVICES_EXT_UDP (pare-feu) Laissez ce champ vide à moins que vous utilisiez un service UDP auquel on doit pouvoir accéder de l'extérieur. Les services qui utilisent UDP comprennent des serveurs DNS, IPSec, TFTP, DHCP et d'autres. Dans ce cas, ajoutez ici les ports UDP requis.

FW_SERVICES_INT_TCP (pare-feu) Avec cette variable, vous définissez les services disponibles pour le réseau interne. La notation est analogue à celle employée pour FW_SERVICES_EXT_TCP, mais les réglages sont cette fois appliqués au réseau *interne*. Cette variable ne doit être configurée que si FW_PROTECT_FROM_INTERNAL a été activée (valeur yes.

FW_SERVICES_INT_UDP (pare-feu) Voir FW_SERVICES_INT_TCP.

La configuration est à présent terminée. N'oubliez pas de tester le pare-feu. En tant qu'utilisateur root, appelez la commande SuSEfirewall2 start pour créer les règles. Utilisez par exemple telnet de l'extérieur, pour vérifier si cette connexion est refusée *de facto* : vous devriez alors voir dans le fichier /var/log/messages des lignes similaires à celles-ci :

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0 OUT=
MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF
PROTO=TCP SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0 OPT
(020405B40402080A061AFEBC0000000001030300)
```

nmap ou nessus sont d'autres paquetages disponibles pour tester la configuration de votre pare-feu. Vous trouverez la documentation relative à nmap dans /usr/share/doc/packages/nmap et celle de nessus dans le répertoire /usr/share/doc/packages/nessus-core après avoit installé le paquetage respectif.

34.1.5 Informations complémentaires

Vous trouverez les informations les plus récentes et de la documentation sur le paquetage SuSEfirewall2 dans /usr/share/doc/packages/

SuSEfirewall2. http://www.netfilter.org est la page d'accueil des projets netfilter/iptables. Vous y trouverez de la documentation en abondance en différentes langues.

34.2 SSH – travailler en réseau en toute sécurité

Lorsque l'on travaille en réseau, il est souvent nécessaire d'accéder à des systèmes depuis des ordinateurs distants. L'utilisateur doit alors s'identifier en envoyant son login et son mot de passe. Si ces données sensibles sont transmises en clair elles risquent d'être interceptées à tout moment par des tiers et d'être utilisées dans l'intérêt de ces derniers en exploitant l'accès de l'utilisateur à son insu. Indépendamment du fait que les attaquants peuvent ainsi prendre connaissance de l'ensemble des données privées de l'utilisateur, ils peuvent utiliser l'accès ainsi obtenu pour attaquer à partir de là d'autres systèmes ou pour usurper les comptes administrateur ou root sur le système visé. Dans le passé, c'était le programme telnet, dépourvu de mécanisme de chiffrement ou de sécurité contre l'écoute des liaisons, qui était utilisé pour connecter deux machines distantes. De même, d'autres canaux de communication, comme les connexions FTP simples et certaines copies entre machines distantes, ne sont pas protégées.

Le programme SSH apporte la protection requise en chiffrant les données d'authentification (généralement un nom d'utilisateur et un mot de passe) ainsi que les autres données échangée. Même s'il reste possible, pour un tiers, d'intercepter les données transmises, leur contenu ne peut pas être déchiffré, faute de disposer de la clé appropriée. Cette méthode permet ainsi des communications sécurisées sur des réseaux non sécurisés tels que le réseau Internet. SUSE LINUX propose pour cela le paquetage OpenSSH.

34.2.1 Le paquetage OpenSSH

Le paquetage OpenSSH est installé par défaut sous SUSE LINUX. Vous disposez ainsi des programmes ssh, scp et sftp, afin de remplacer telnet, rlogin, rsh, rcp et ftp. Dans la configuration par défaut, l'accès à un système SUSE LINUX n'est possible qu'avec les utilitaires OpenSSH et uniquement si le pare-feu autorise l'accès.

34.2.2 Le programme ssh

Le programme ssh permet de se connecter à un système distant et d'y travailler de façon interactive. Il constitue ainsi une alternative à telnet et à rlogin. Le programme slogin n'est qu'un lien symbolique faisant référence à ssh. Ainsi, la commande `ssh soleil` permet de se connecter sur la machine soleil. L'hôte invite alors à entrer le mot de passe pour le système soleil.

Une fois authentifié, vous pouvez alors y travailler soit à partir de la ligne de commande soit en mode graphique, par exemple avec YaST. Dans le cas où votre nom d'utilisateur sur la machine locale et celui sur le système distant sont différents, vous pouvez spécifier un autre nom, par exemple `ssh -l augustine soleil` ou `ssh augustine@soleil`.

D'autre part, le programme ssh offre une possibilité connue avec rsh et consistant à exécuter des commandes sur un autre système. Dans l'exemple suivant, la commande `uptime` est exécutée sur la machine soleil et un répertoire nommé `tmp` est créé. Le programme affiche sur le terminal local de la machine terre.

```
ssh soleil "uptime; mkdir tmp"
tux@soleil's password:
1:21pm  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

Dans cette commande, les guillemets sont requis afin de regrouper les deux instructions en une commande unique. C'est nécessaire pour permettre l'exécution de la seconde commande sur la machine soleil.

34.2.3 scp—Copie sécurisée

Le programme scp vous permet de copier des fichiers sur une machine distante. scp constitue une alternative sécurisée et chiffrée au programme rcp. Ainsi, la commande `scp MonCourrier.tex soleil:` copie le fichier `MonCourrier.tex` de la machine terre sur la machine soleil. Dans le cas où le nom d'utilisateur sur terre est différent de celui sur soleil, utilisez pour la commande scp la notation `NomUtilisateur@NomMachine`. L'option `-l` n'est pas disponible.

Après avoir saisi votre mot de passe, le programme scp commence à transférer les données en affichant l'avancement à l'aide d'une jauge formée d'astérisques et progressant de gauche à droite. Dans le même temps, la durée estimée restant jusqu'à la fin de la transmission (estimated time of arrival) est affichée sur la droite. Il est également possible d'inhiber l'affichage à l'aide de l'option `-q`.

La copie de fichiers individuels n'est pas la seule opération que scp permet d'effectuer. En effet, il est également possible de transférer récursivement des répertoires entiers : ainsi, la commande `scp -r src/ soleil:backup/` copie la totalité du répertoire `src/`, y compris les sous-répertoires présents sur la machine soleil, dans le sous-répertoire `backup/`. Ce dernier est créé automatiquement s'il n'existe pas encore.

L'option `-p` permet à scp de conserver l'horodatage des fichiers. L'option `-C` permet de compresser les fichiers à transférer, ce qui, d'un côté, permet de réduire le volume de données à transférer, mais de l'autre, impose une charge supérieure au système.

34.2.4 sftp—Transfert de fichiers sécurisé

On peut aussi utiliser le programme sftp pour transférer les données de façon sécurisée. sftp propose une session à l'intérieur de laquelle on peut utiliser plusieurs des commandes ftp bien connues. Par rapport à scp, le principal avantage est de pouvoir transférer des données lorsqu'on ne connaît pas le nom de fichier.

34.2.5 Le démon SSH (sshd)—côté serveur

Pour pouvoir fonctionner, ssh et scp, les programmes clients du paquetage SSH ont besoin que le démon SSH qui est un serveur s'exécute en arrière-plan. Celui-ci attend les connexions sur le `port TCP/IP numéro 22`. La première fois qu'il est démarré, le démon génère trois paires de clés. Celles-ci comportent une partie privée et une partie publique (public). il s'agit donc d'une méthode à clé publique. Pour assurer la sécurité de l'application à l'aide de SSH, seul l'administrateur doit pouvoir voir les fichiers de la clé privée. Les privilèges correspondant sont définis par défaut de manière restrictive. Les clés privées sont utilisées en local uniquement par le démon SSH et ne doivent être communiquées à personne. En revanche, la partie publique de la clé (identifiable par l'extension de fichier `.pub`) peut être communiquée à vos correspondants et peut être lue par tous les utilisateurs.

Une connexion est créée par le client SSH. Le démon SSH en attente et le client SSH à l'origine de la demande échangent des données d'identification en vue de comparer la version du protocole et du logiciel et d'éviter une connexion sur un mauvais port. La réponse étant apportée par un processus fils du démon SSH initial, il est possible d'avoir plusieurs connexions SSH simultanément.

Afin d'assurer la communication entre le serveur SSH et le client SSH, le programme OpenSSH prend en charge les versions 1 et 2 du protocole SSH. Après avoir réinstallé SUSE LINUX, c'est la version 2 actuelle du protocole qui est automatiquement utilisée. Si vous souhaitez continuer à utiliser SSH1 après une mise à jour, veuillez suivre les instructions données dans `/usr/share/doc/packages/openssh/README.SuSE`. Vous y trouverez également la marche à suivre pour passer d'un environnement SSH 1 à un environnement SSH 2 opérationnel.

Si vous utilisez le protocole SSH version 1, le serveur envoie sa clé d'hôte (en anglais, host key) publique ainsi qu'une clé de serveur (en anglais, server key) générée toutes les heures par le démon SSH. Grâce à ces deux clés, le client SSH chiffre une clé de session (en anglais, session key) et l'envoie au serveur SSH.Il communique par ailleurs au serveur la méthode de chiffrement choisie.

Le protocole SSH version 2 fonctionne sans la clé de serveur. Ce dispositif est remplacé par un algorithme de Diffie-Hellman destiné à l'échange des clés.

Il n'est pas possible de déduire les clés privées de l'hôte et du serveur, indispensables pour déchiffrer la clé de session, à partir des parties publiques de la clé. Ainsi, seul le démon SSH contacté est en mesure de déchiffrer la clé de session à l'aide de ses clés privées (voir `man /usr/share/doc/packages/openssh/RFC.nroff`). Cette phase préparatoire de la connexion peut être aisément tracée à l'aide de l'option de débogage `-v` du programme client SSH.

Par défaut, c'est la version 2 du protocole SSH qui est utilisée, même si le paramètre `-1` permet d'imposer la version 1 du protocole SSH. En stockant après le premier contact toutes les clés publiques dans `~/.ssh/known_hosts`, il est possible de contrer les attaques de type interception (man-in-the-middle). Les serveurs SSH tentant d'usurper le nom et l'adresse IP d'un autre sont démasqués avec un avertissement sans ambiguïté. Ils sont identifiés par leur clé d'hôte différente de `~/.ssh/known_hosts` ou sont dans l'impossibilité de déchiffrer la clé de session convenue, faute de connaître la partie privée adéquate.

Il est recommandé d'archiver sur un support externe et en les protégeant comme il se doit les clés privées et publiques de `/etc/ssh/`. Vous pouvez ainsi constater d'éventuelles modifications apportées aux clés et récupérer les anciennes clés dans le cas où vous auriez à réinstaller votre système. Cette précaution épargnera aux utilisateurs l'inquiétude que peuvent causer des messages d'avertissement. Dans le cas où vous avez la certitude d'avoir à faire au bon serveur SSH en dépit de l'avertissement, la ligne correspondante doit être retirée du fichier `~/.ssh/known_hosts`.

34.2.6 Mécanismes d'authentification de SSH

L'authentification proprement dite intervient à cet instant. Sous sa forme la plus simple, elle consiste à saisir un mot de passe, de manière analogue à la procédure illustrée dans les exemples précédents. L'objet de SSH était de mettre en place un logiciel sécurisé tout en restant simple à utiliser. De manière analogue aux programmes rsh et rlogin à remplacer, il importe donc que SSH offre une méthode d'authentification simple à utiliser au quotidien. Cet objectif est réalisé par SSH à l'aide d'une autre paire de clés générée ici par l'utilisateur. Le paquetage SSH offre pour cela l'utilitaire ssh-keygen. La paire de clés est générée après avoir saisi `ssh-keygen -t rsa` ou `ssh-keygen -t dsa` et vous devez indiquer un nom pour le fichier de base destiné à stocker les clés.

Validez la valeur par défaut et lorsque l'on vous demande une phrase de passe, donnez-en une. Même si le logiciel accepte une phrase de passe vide, nous conseillons de choisir un texte de 10 à 30 signes. Dans la mesure du possible, évitez d'utiliser des mots ou phrases courts et simples. Après la saisie, vous devez vérifier la première saisie en effectuant une seconde saisie. Vous devez ensuite indiquer l'emplacement de la clé privée et publique, en l'occurrence les fichiers `id_rsa` et `id_rsa.pub`.

Utilisez la commande `ssh-keygen -p -t rsa` ou `ssh-keygen -p -t dsa` pour modifier votre ancienne phrase de passe. Copiez la partie publique de la clé (dans notre exemple `id_rsa.pub`) sur la machine distante et enregistrez-la sous `~/.ssh/authorized_keys`. Lors de la prochaine connexion, vous devrez saisir votre phrase de passe. Dans le cas contraire, vérifiez l'emplacement et le contenu des fichiers dont il vient d'être question.

À la longue, cette procédure s'avère plus lourde que celle consistant à saisir un mot de passe. Le paquetage SSH s'accompagne d'un utilitaire supplémentaire, ssh-agent, proposant des clés privées valables pour la durée d'une session X. Pour cela, le programme X est démarré comme processus fils de ssh-agent. La méthode la plus simple pour mettre cette fonctionnalité en place consiste à placer au début du fichier `.xsession` la variable `usessh` en fixant sa valeur à `yes` et à vous connecter à partir d'un gestionnaire de connexions tel que KDM ou XDM. Une autre possibilité est d'entrer `ssh-agent startx`.

Vous pouvez à présent utiliser `ssh` ou `scp` comme à l'accoutumée. Si vous avez partagé votre clé publique comme indiqué précédemment, vous devriez être dispensé de donner votre mot de passe. Lorsque vous vous éloignez de votre ordinateur, prenez toutefois la précaution de terminer votre session X ou de la verrouiller à l'aide d'un économiseur d'écran protégé par mot de passe, par exemple xlock.

Toutes les modifications importantes résultant de l'utilisation du protocole SSH version 2 sont également récapitulées dans le fichier /usr/share/doc/packages/openssh/README.SuSE.

34.2.7 Mécanismes de redirections, d'authentification et X

Indépendamment des améliorations en matière de sécurité dont il vient d'être question, le programme ssh facilite également l'utilisation d'applications X distantes. Lorsque vous appelez ssh avec l'option -X, la variable DISPLAY est automatiquement définie sur le système distant et toutes les sorties X sont redirigées vers la machine source à travers la connexion ssh existante. Cette fonctionnalité pratique interdit dans le même temps les possibilités d'écoute qui existaient auparavant, lorsque l'on appelait à distance des applications X pour les afficher en local.

En définissant l'option -A, le mécanisme d'authentification de l'agent ssh-agent est repris sur la machine suivante. Vous pouvez ainsi passer d'une machine à l'autre sans être obligé de saisir de mot de passe. Ceci n'est toutefois possible que si vous avez préalablement copié et convenablement enregistré votre clé publique sur les machines cibles concernées.

Par précaution, les deux mécanismes sont désactivés par défaut, même s'ils peuvent être activés de manière permanente dans le fichier de configuration système /etc/ssh/ssh_config ou dans le fichier utilisateur ~/.ssh/config.

Le programme ssh peut également être utilisé afin de permettre des redirections de connexions TCP/IP. Exemple d'application : la redirection des ports SMTP et POP3 :

```
ssh -L 25:soleil:25 terre
```

Dans cet exemple, toutes les connexions vers *terre port 25* (SMTP) sont redirigées vers le port SMTP de soleil via un canal chiffré. Cette possibilité est particulièrement utile pour les utilisateurs de serveurs SMTP dépourvus de fonctions SMTP-AUTH ou POP-before-SMTP. Ainsi, le courrier peut être transmis de n'importe quel endroit disposant d'une connexion réseau afin d'être acheminé par le serveur de messagerie domestique. De manière analogue, la commande suivante permet de rediriger toutes les requêtes POP3 (port 110) adressées à terre vers le port POP3 de soleil :

```
ssh -L 110:soleil:110 terre
```

Vous devez exécuter ces deux exemples en tant qu'utilisateur `root`, la connexion s'effectuant sur des ports locaux privilégiés. Lorsque la connexion SSH est établie, l'utilisateur envoie et reçoit les messages à partir de son compte habituel. L'hôte SMTP et POP3 doit être configuré à `localhost`. Vous trouverez des informations complémentaires dans les pages de manuels des différents programmes et dans les fichiers sous `/usr/share/doc/packages/openssh`.

34.3 Chiffrer des partitions et des fichiers

34.3.1 Scénarios d'utilisation

Chaque utilisateur possède certaines données confidentielles auxquelles les tiers ne sont pas censés pouvoir accéder. Plus vous travaillez en réseau et plus vous vous déplacez souvent, plus vous devriez être méfiant à propos de vos données. Le chiffrement des fichiers ou de partitions entières se justifie toujours lorsque les tiers ont accès au système, que ce soit au moyen d'une connexion réseau ou en y accédant physiquement. La liste suivante décrit quelques scénarios d'utilisation que l'on peut envisager.

Ordinateurs portables Si vous voyagez avec votre ordinateur portable, il peut être très judicieux de chiffrer les partitions sur le disque dur qui contient des données confidentielles. Si vous perdez votre ordinateur portable ou si on vous le vole, vos données sont à l'abri des indiscrétions au sein d'un système de fichiers chiffré ou d'un fichier chiffré unique.

Supports amovibles Les clés USB ou les disques durs externes risquent d'être volés, tout comme les ordinateurs portables. Un système de fichiers chiffré vous offre une protection contre les tiers dans ces cas.

34.3.2 Configurer avec YaST un système de fichiers chiffré

YaST propose de chiffrer des fichiers ou des partitions aussi bien pendant l'installation que sur un système déjà installé. On peut toujours créer un fichier chiffré, car il s'intègre sans problème à un schéma de partitionnement existant. Pour chiffrer une partition entière, vous devez dédier une partition à cet effet dans le schéma de partitionnement. La proposition de partitionnement standard telle que la suggère YaST ne prévoit pas, par défaut, de partition chiffrée. Ajoutez-la à la main dans la boîte de dialogue de partionnement.

Créer une partition chiffrée pendant l'installation

> **Avertissement**
>
> **Saisie du mot de passe**
>
> Observez les avertissements sur la sécurité du mot de passe lorsque vous créez le mot de passe des partitions chiffrées et retenez-le bien. Sans le mot de passe, il est impossible d'accéder aux données chiffrées.
>
> **Avertissement**

La boîte de dialogue de partitionnement en mode expert décrite dans la section 2.7.5 page 75 offre les options nécessaires pour créer une partition chiffrée. Cliquez sur 'Créer' comme lors de la création d'une partition normale. Dans la boîte de dialogue qui apparaît, saisissez les paramètres de partitionnement de la nouvelle partition, tels que le type de formatage et le point de montage souhaités. Terminez la création en cliquant sur 'Système de fichiers crypté'. Dans la boîte de dialogue suivante, définissez le mot de passe et répétez-le pour des raisons de sécurité. La nouvelle partition chiffrée est créée dès que la boîte de dialogue de partitionnement est achevée en cliquant sur 'OK'. Le système d'exploitation demande ce mot de passe à l'utilisateur lors de l'amorçage, avant que la partition ne puisse être montée.

Si vous ne souhaitez pas monter la partition chiffrée au cours du démarrage, appuyez sur Entrée lorsque vous êtes invité à saisir le mot de passe. Puis déclinez l'offre de saisir le mot de passe à nouveau. Le système de fichiers chiffré n'est pas monté dans ce cas et le système d'exploitation continue à amorcer, ce qui est le moyen le plus sûr de protéger vos données. La partition est à la disposition de tous les utilisateurs une fois qu'elle a été montée.

Si le système de fichiers chiffré ne doit être montré que quand c'est nécessaire, cochez'Ne pas monter au démarrage du système' dans la boîte de dialogue 'Options Fstab'. La partition correspondante ne sera pas montée pendant le démarrage du système. Pour la mettre à disposition par la suite, montez-la manuellement avec `mount` ⟨*nom_de_la_partition*⟩ ⟨*point_de_montage*⟩. Saisisez le mot de passe lorsque vous êtes invité à monter la partition. Lorsque vous en avez terminé avec cette partition, démontez-la avec `umount nom_de_la_partition` pour éviter que d'autres utilisateurs ne puissent y obtenir accès.

Créer une partition chiffrée sur un système en cours de fonctionnement

Avertissement

Activer le chiffrement sur un système en cours de fonctionnement

Il est également possible de créer des partitions chiffrées sur un système en cours de fonctionnement, de la même manière que pendant l'installation. Toutefois, le chiffrement d'une partition existante détruit toutes les données qu'elle contient.

Avertissement

Sur un système en cours de fonctionnement, choisissez 'Système' → 'Partitionnement'

dans le Centre de Contrôle de YaST. Cliquez sur 'Oui' pour continuer. Au lieu de choisir 'Créer', comme mentionné ci-dessus, cliquez sur 'Modifier'. Le reste de la procédure est identique.

Installer des fichiers chiffrés

Tout comme on peut utiliser une partition, il est possible de créer des systèmes de fichiers chiffrés à l'intérieur de fichiers séparés qui contiendront des données confidentielles. Ceux-ci sont créés à partir de la même boîte de dialogue de YaST. Choisissez 'Fichier de chiffrement' et saisissez le chemin du fichier à créer ainsi que sa taille prévue. Acceptez les paramètres proposés pour le type de formatage et le type de système de fichiers. Indiquez ensuite le point de montage et décidez si le système de fichiers chiffré devra être monté au cours de l'amorçage.

Les fichiers chiffrés présentent l'avantage de pouvoir être ajoutés sans modification du partitionnement du disque dur. Ils sont montés comme un périphérique virtuel (loop device) et se comportent alors comme des partitions normales.

Utilisation de vi pour chiffrer des fichiers

L'utilisation de partitions chiffrées présentent un inconvénient : pendant que cette partition est montée, l'utilisateur `root`, au moins, peut accéder aux données. Pour éviter cette situation, il est possible d'utiliser vi en mode chiffré.

Utilisez `vi -x nom_de_fichier` pour éditer un nouveau fichier. vi vous demandera un mot de passe puis chiffrera le contenu du fichier. Lorsque vous accéderez à nouveau à ce fichier, vi vous demandera le mot de passe correct.

Pour une sécurité encore plus importante, vous pouvez mettre votre fichier texte chiffré dans une partition déjà sécurisée. Ceci est utile car le mécanisme de chiffrement utilisé dans vi est connu pour ne pas être très solide.

34.3.3 Chiffrer le contenu de supports amovibles

Les supports amovibles, comme les disques dur externes ou les clés USB sont reconnus par YaST comme tout autre disque dur. Il est possible de chiffrer des fichiers ou des partitions sur de tels supports en procédant comme décrit ci-dessus. Ne choisissez pas de monter ces supports pendant l'amorçage, car il ne sont en principe mis en place qu'au cours du fonctionnement du système.

34.4 Sécurité et confidentialité

L'une des caractéristiques principales d'un système Linux/Unix est que plusieurs utilisateurs peuvent simultanément (multiuser) effectuer plusieurs tâches sur le même ordinateur (multitasking). En outre, le réseau est transparent au système d'exploitation, si bien que, très souvent, les utilisateurs ne savent pas si les données ou les applications qu'ils utilisent se trouvent en local sur leur ordinateur ou leur sont fournies par le réseau.

Pour que plusieurs utilisateurs puissent travailler sur un même système, leurs données doivent pouvoir être gérées de manière séparée. Il s'agit ici, entre autres, de considérations relatives à la sécurité et à la protection de la vie privée. La sûreté des données était déjà importante quand les ordinateurs n'étaient pas encore en réseau. Tout comme aujourd'hui, le plus important était de pouvoir conserver les données malgré la perte ou la défaillance du support de données, généralement, le disque dur.

Même si cette section concerne principalement la confidentialité des données et la protection de la vie privée de l'utilisateur, il faut insister sur le fait qu'une politique de sécurité globale doit toujours comprendre, en tant que partie intégrante du système, un système de sauvegarde régulier, éprouvé et qui fonctionne correctement. Sans cette sauvegarde des données, il serait très difficile d'accéder à nouveau aux données non seulement dans le cas d'une défaillance du matériel, mais également lorsque l'on soupçonne que quelqu'un a réussi à accéder aux données de manière illégale.

34.4.1 Sécurité locale et sécurité du réseau

Il existe plusieurs possibilités pour accéder aux données :

- la communication avec quelqu'un qui a accès aux informations souhaitées ou qui a accès aux données d'un ordinateur,
- directement depuis la console d'un ordinateur (accès physique),
- à travers une ligne série
- en utilisant un lien réseau

Dans tous ces cas de figure, un utilisateur devrait être authentifié avant d'obtenir l'accès aux ressources ou aux données. Un serveur web peut être moins restrictif à ce sujet, néanmoins vous ne souhaitez très certainement pas que le serveur web révèle toutes vos informations personnelles à n'importe quel internaute.

Le premier des cas mentionnés ci-dessus est celui qui fait le plus appel au facteur humain, comme dans une banque où vous devez fournir à un employé autorisé à accéder à votre compte une signature, un numéro d'identification personnel ou un mot de passe, pour prouver que vous êtes bien la personne que vous affirmez être. La plupart du temps, cela peut se faire en mentionnant certaines connaissances ou en obtenant, par la ruse ou en faisant preuve de rhétorique, la confiance d'une personne détenant les connaissances nécessaires, pour que cette personne communique d'autres informations, parfois à l'insu de la victime. Dans le monde des pirates, on parle de *social engineering* (ingénierie sociale). Contre ce type d'attaque, la seule solution consiste à éduquer les personnes et à manipuler avec précaution vos informations et à tenir votre langue. Les effractions dans les systèmes informatiques sont souvent précédées d'une tentative d'attaque d'ingénierie sociale dirigée contre le personnel d'accueil, les prestataires de service de la société ou les membres de la famille et qui n'est décelée, la plupart du temps, que beaucoup plus tard.

Quelqu'un qui souhaite accéder aux données de manière illégale pourrait très bien aussi utiliser la méthode traditionnelle et attaquer directement le matériel. L'ordinateur doit donc être protégé contre les vols, les échanges et les sabotages partiels ou totaux. Ceci concerne aussi la sauvegarde des données et un éventuel câble de connexion réseau ou électrique. En outre, la procédure d'amorçage doit être sécurisée car des combinaisons de touches connues peuvent entraîner des réactions spéciales de l'ordinateur. Le fait de définir des mots de passe pour le BIOS et le gestionnaire d'amorçage protège contre de telles tentatives.

Les interfaces série avec des terminaux série sont toujours très largement utilisés de nos jours. À la différence des interfaces réseau, elles ne s'appuient pas sur un protocole réseau pour communiquer avec l'hôte. Un simple câble ou un port infrarouge est utilisé comme moyen de transmission pour les signaux simples.Le

câble même est ainsi le point d'attaque le plus simple à utiliser : il suffit d'y connecter une vieille imprimante pour enregistrer la communication. Ce qui peut être fait avec une imprimante peut également être réalisé d'autres façons qui dépendent de l'effort fourni par l'attaquant.

La lecture locale d'un fichier sur un ordinateur implique d'autres règles d'accès que l'ouverture d'une connexion réseau avec un serveur sur un hôte différent. Il est nécessaire de bien distinguer entre sécurité locale et sécurité réseau. La ligne de séparation est le point où les données doivent être mises en paquets pour pouvoir être envoyées et utilisées.

Sécurité locale

La sécurité locale commence par l'environnement physique dans lequel l'ordinateur est installé. Installez votre ordinateur de manière dans un endroit où le niveau de sécurité correspond à vos besoins et à vos exigences. L'objectif principal de la sécurité locale consiste à séparer les différents utilisateurs les uns des autres de manière à ce qu'aucun utilisateur ne puisse s'accaparer les droits ou l'identité d'un autre utilisateur. Cela s'applique dans tous les cas, et en particulier, naturellement, aux droits de l'utilisateur `root` qui possède les pleins pouvoirs dans le système ; il peut notamment, sans mot de passe, prendre l'identité de n'importe quel utilisateur local et lire tous les fichiers locaux.

Mots de passe

Votre système Linux n'enregistre pas les mots de passe en texte clair pour ensuite comparer le mot de passe saisi avec celui qui est enregistré. En cas de vol du fichier dans lequel sont enregistrés les mots de passe, tous les comptes de votre système seraient compromis. Au contraire, votre mot de passe est enregistré sous sa forme chiffrée et à chaque fois que vous saisissez votre mot de passe, il est à nouveau chiffré et le résultat est comparé avec ce qui est enregistré en tant que mot de passe chiffré. Cela n'a naturellement un sens que s'il n'est pas possible de calculer le mot de passe en clair à partir du mot de passe chiffré.

On utilise à cet effet un algorithme spécial, appelé *algorithme à trappe* parce qu'il ne fonctionne que dans un sens. Un attaquant ayant pris possession du mot de passe chiffré ne peut pas simplement calculer et obtenir le mot de passe, il doit en revanche essayer toutes les combinaisons de caractères possibles pour un mot de passe pour trouver une combinaison qui une fois codée ressemble au mot de passe qu'il détient. Avec des mots de passe de huit lettres, il existe un nombre considérable de combinaisons possibles.

L'un des arguments pour la sécurité de cette méthode dans les années 70 était que l'algorithme utilisé était particulièrement lent et qu'il fallait plusieurs secondes pour chiffrer un mot de passe. Cependant, les ordinateurs actuels peuvent sans effort réaliser de plusieurs centaines de milliers à plusieurs millions de chiffrements par seconde. C'est pour cette raison que les mots de passe chiffrés ne doivent pas être visibles de tous les utilisateurs (un utilisateur normal ne peut pas lire `/etc/shadow`) et les mots de passe ne doivent pas être faciles à deviner dans le cas où les mots de passe chiffrés deviendraient lisibles suite à une erreur. Il n'est pas très utile de "transformer" un mot de passe tel que "tantelise" en "t@nt31ls3".

Le remplacement de certaines lettres d'un mot par des chiffres leur ressemblant n'est pas très sûr et peut facilement être déchiffré par des programmes de craquage qui utilisent des dictionnaires. Il est préférable d'utiliser des combinaisons de lettres qui ne constituent pas un mot connu et qui n'ont une signification personnelle que pour l'utilisateur, comme les premières lettres des mots d'une phrase ou par exemple un titre de livre comme "Le nom de la rose d'Umberto Eco". Vous pourriez ainsi obtenir un bon mot de passe : "LNdlRdUE9". Un mot de passe tel que "bonvin" ou "Jasmin76" pourrait facilement être deviné par quelqu'un vous connaissant ne serait-ce que superficiellement.

Le processus d'amorçage

Configurez votre système de façon à interdire tout démarrage à partir d'une disquette ou d'un CD en supprimant les lecteurs correspondants ou en définissant un mot de passe du BIOS et en n'autorisant dans le BIOS que l'amorçage à partir du disque dur. Généralement, les systèmes Linux démarrent avec un gestionnaire de démarrage qui permet de passer des options supplémentaires au noyau à démarrer. Interdisez aux autres l'utilisation de ces paramètres en configurant un mot de passe supplémentaire dans `/boot/grub/menu.lst` (voir le chapitre 8 page 183). Ces options sont périlleuses en termes de sécurité car non seulement le noyau s'exécute avec les droits de l'utilisateur `root` mais il est la première autorité qui offre, dès l'amorçage, les droits de l'utilisateur `root`.

Droits d'accès

Un principe général consiste à toujours travailler avec les privilèges les plus bas possibles pour une tâche donnée. Il n'est effectivement absolument pas nécessaire de lire et d'écrire son courrier en tant que `root`. Si le programme de messagerie que vous utilisez comporte un bogue, celui-ci peut être exploité pour une attque

qui agit alors avec exactement les droits que vous aviez au moment de l'accès au profgramme. En suivant le principe énoncé ici, vous pouvez limiter les dégâts.

Les droits individuels des plus de 200 000 fichiers d'une distribution SUSE sont attribués avec soin. L'administrateur d'un système ne doit installer de logiciels supplémentaires ou d'autres fichiers qu'avec la plus grande précaution et faire particulièrement attention aux droits attribués aux fichiers. Les administrateurs expérimentés et soucieux de la sécurité utilisent toujours l'option `-l` de la commande `ls` pour obtenir une liste complète des fichiers et de leurs droits d'accès afin de pouvoir reconnaître immédiatement les droits de fichiers mal définis. Un attribut mal défini ne signifie pas seulement que les fichiers peuvent être modifiés ou supprimés, mais également que les fichiers modifiés peuvent être exécutés par l'utilisateur `root` ou, dans le cas de fichiers de configuration de programmes, utilisés en tant qu'utilisateur `root`. Cela permettrait à un attaquent d'augmenter ses possibilités de façon considérable. On appelle ce genre d'attaque des œufs de coucou parce que le programme (l'œuf) est exécuté (couvé) par un utilisateur étranger (l'oiseau), un peu comme un coucou se débrouille pour faire couver ses œufs par d'autres oiseaux.

Les systèmes SUSE LINUX disposent des fichiers `permissions`, `permissions.easy`, `permissions.secure` et `permissions.paranoid` dans le répertoire `/etc`. Dans ces fichiers sont définis des droits importants tels que les répertoires dans lesquels tout utilisateur a des droits d'écriture, ou les bits "setuser ID" des fichiers. Ces bits de changement d'identité font qu'un programme ne s'exécute pas avec les droits du propriétaire du processus qui l'a démarré mais avec les droits du propriétaire du fichier, et c'est généralement l'utilisateur `root`). L'administrateur dispose du fichier `/etc/permissions.local` dans lequel il peut procéder à ses propres modifications.

Vous pouvez également choisir confortablement avec YaST dans l'option de menu 'Sécurité' lequel de ces fichiers sera utilisé par les programmes de configuration de SUSE pour l'attribution des droits. Vous trouverez plus d'informations à ce sujet directement dans le fichier `/etc/permissions` et la page de manuel de la commande `chmod` (`man chmod`).

Débordements de tampon et bogues dans des chaînes de format

À chaque fois qu'un programme traite des données qui se trouvent ou se trouvaient sous le contrôle d'un utilisateur dans un format donné, nous vous recommandons la plus grande vigilance. Le programmeur de l'application aussi doit faire preuve de vigilance : il doit s'assurer que les données sont correctement interprétées par le programme, qu'elles n'ont à aucun moment été écrites dans un

espace mémoire trop petit et qu'il transmet les données d'une manière cohérente à l'aide de son propre programme et des interfaces définies à cet effet.

Il y a *débordement de tampon* (buffer overflow) quand, lors de l'écriture à l'intérieur d'une mémoire tampon, on ne fait pas attention à la taille réelle du tampon. Il se peut que les données (qui proviennent de l'utilisateur) nécessitent un peu plus de place que disponible dans le tampon. Avec ce débordement de tampon au delà de ses capacités, il se peut qu'un programme, du fait des données qu'il doit en théorie seulement traiter, exécute des morceaux de code choisis par l'utilisateur et non par le programmeur. Il s'agit d'une erreur grave notamment quand le programme fonctionne avec des droits particuliers voir la section Droits d'accès page 652).

Les *bogues dans les chaînes de format* fonctionnent quelque peu différemment mais à nouveau les données saisies par l'utilisateur peuvent détourner le programme de sa vocation d'origine. Ces erreurs de programmation sont normalement exploitées par les programmes exécutés avec des privilèges élevés, comme par exemple les programmes setuid et setgid. Vous pouvez donc vous protéger ainsi que votre système contre ce type d'erreurs en éliminant les droits d'exécution particuliers des programmes. Ici aussi s'applique donc le principe des privilèges les plus restreints possibles (voir la section Droits d'accès page 652).

Comme les débordements de tampon et les bogues dans les chaînes de format sont des erreurs qui se présentent lors du traitement des données utilisateur, elles ne sont pas nécessairement exploitables uniquement quand on dispose déjà d'un accès à un login local. Beaucoup des erreurs connues peuvent être exploitées par l'intermédiaire d'une connexion réseau. C'est pour cette raison que l'on ne peut pas associer les débordements de tampon et les bogues dans les chaînes de format directement à l'ordinateur local ou au réseau.

Virus

Contrairement à ce que l'on croit généralement, il existe aussi des virus pour Linux. Cependant, les virus connus ont été créés par leurs auteurs en tant que *proof of concept*, à savoir une démonstration du bien-fondé d'une technique. Aucun de ces virus n'a encore été observé *dans la nature*.

Pour se propager, les virus ont besoin d'un hôte sans lequel ils ne peuvent survivre. Cet hôte est un programme ou un emplacement sur le disque important pour le système, comme par exemple l'enregistrement d'amorçage maître et le code de programme du virus doit pouvoir y écrire. Linux, du fait de ses fonctionnalités multi-utilisateurs, peut limiter l'accès en écriture aux fichiers et notamment aux fichiers système. Si vous travaillez en tant qu'utilisateur `root` vous

augmentez la probabilité d'infecter votre système avec ce type de virus. Si vous observez cependant la règle des privilèges les plus restreints possibles, il devient difficile d'être infecté par un virus sous Linux.

En outre, vous ne devriez jamais exécuter à la légère un programme que vous avez récupéré sur l'Internet et dont vous ne connaissez pas l'origine. Les paquetages rpm SUSE portent une signature cryptographique et témoignent avec cette signature numérique du soin apporté par SUSE lors de l'élaboration de ses paquetages. Les virus sont l'un des symptômes classiques d'un système hautement sécurisé devenu non sûr lorsque l'administrateur ou même l'utilisateur n'ont pas une parfaite conscience de la sécurité.

Il ne faut pas confondre les virus avec les vers qui sont également des phénomènes de la sécurité réseau mais qui n'ont en revanche pas besoin d'hôte pour se propager.

Sécurité réseau

Dans le domaine de la sécurité locale il fallait séparer les utilisateurs travaillant sur le même ordinateur, notamment l'utilisateur `root`. En matière de sécurité réseau, en revanche, c'est l'intégralité du système qu'il faut protéger contre les attaques en provenance du réseau. L'authentification des utilisateurs dans le cas de la connexion classique avec un nom d'utilisateur et un mot de passe relève de la sécurité locale. En cas de connexion par le réseau, il faut différencier les deux aspects de la sécurité : avant la réussite de l'authentification, on parle de sécurité réseau, après le login, il s'agit de sécurité locale.

Système X Window et authentification X11

Comme déjà mentionné précédemment, la transparence du réseau est une caractéristique fondamentale d'un système Unix. Avec X11, le système de fenêtrage d'Unix, cela l'est au plus haut point ! Vous pouvez ainsi simplement vous connecter à un ordinateur distant et y démarrer un programme qui s'affichera alors via le réseau sur votre ordinateur.

Si un client X doit être affiché via le réseau sur notre serveur X, alors le serveur doit protéger la ressource qu'il gère (l'affichage) contre les accès non autorisés. Concrètement, cela signifie ici que le programme client doit obtenir des droits. Pour X Window, cela se passe de deux manières différentes : un contrôle d'accès fondé sur un ordinateur ou sur un cookie. Le premier se fonde sur l'adresse IP de l'ordinateur sur lequel le programme client doit être exécuté et est contrôlé avec

le programme xhost. Le programme xhost inscrit une adresse IP d'un client légitime dans une mini-base de données sur le serveur X. Une authentification uniquement fondée sur une adresse IP n'est cependant pas considérée comme sûre. Il pourrait très bien y avoir un deuxième utilisateur actif sur l'ordinateur avec le programme client et celui-ci aurait, comme quiconque qui déroberait l'adresse IP, accès au serveur X. C'est pour cette raison qu'il est inutile d'aller plus loin au sujet de ces méthodes. Les pages du manuel obtenues avec la commande `xhost` donnent davantage d'explications sur leur fonctionnement.

Dans le cas d'un contrôle d'accès fondé sur un cookie, une chaîne de caractères connue uniquement par le serveur X et l'utilisateur connecté de manière légitime est utilisée comme preuve d'identité, un peu à l'instar d'un mot de passe. Ce cookie (le mot anglais cookie signifie biscuit et désigne ici les biscuits porte-bonheur chinois qui contiennent une maxime) est enregistré dans le fichier `.Xauthority` dans le répertoire personnel de l'utilisateur lors du login et est ainsi à la disposition de chaque client X Window qui souhaite afficher une fenêtre sur le serveur X. Le programme `xauth` fournit à l'utilisateur l'outil pour analyser le fichier `.Xauthority`. Si vous supprimez ou renommez le fichier `.Xauthority` de votre répertoire personnel, vous ne pourrez plus ouvrir d'autres fenêtres ou de nouveaux clients X. Vous trouverez plus d'informations sur les aspects liés à la sécurité de X Window dans la page de manuel de `Xsecurity` (`man Xsecurity`).

SSH (secure shell) peut être utilisé pour chiffrer complètement une connexion réseau et la rediriger vers un serveur X de façon transparente sans que le mécanisme de chiffrement soit perçu par l'utilisateur. Ceci est également appelé redirection X. La redirection X est réalisée en simulant un serveur X du côté du serveur et en définissant une variable DISPLAY pour l'interpréteur de commandes sur l'hôte distant. Vous trouverez plus de détails sur SSH dans la section 34.2 page 640.

Avertissement

Si vous pensez que l'ordinateur auquel vous vous connectez n'est pas sûr, vous ne devez alors pas autoriser la redirection X. Lorsque la redirection X est activée, des attaquants peuvent aussi se connecter en s'authentifiant auprès de votre serveur X via votre connexion SSH et, par exemple, épier votre clavier.

Avertissement

Débordements de tampon et bogues dans les chaînes de format

Comme évoqués dans la section Débordements de tampon et bogues dans des chaînes de format page 653, les débordements de tampon et bogues dans les chaînes de format devraient être considérées comme des thèmes concernant à la fois la sécurité locale et la sécurité en réseau. Comme pour les variantes locales de ces erreurs de programmation, les débordements de tampon des services réseau sont la plupart du temps utilisés pour obtenir les droits de l'utilisateur `root`. Si tel n'est pas le cas, l'attaquant peut alors au moins réussir à accéder à un compte local sans privilèges d'où il pourrait par la suite exploiter les éventuels problèmes de sécurité locale.

Les débordements de tampon et les bogues dans les chaînes de format sont probablement les variantes les plus fréquentes d'attaques distantes exploitables sur le réseau. On trouve sur les listes de diffusion relatives à la sécurité des exploits (des programmes qui utilisent les brèches qui viennent d'être découvertes). Même une personne ne connaissant pas les détails précis de la faille de sécurité peut l'exploiter. L'expérience a montré que la libre disposition des codes d'exploit (exploit codes) a, de manière générale, amélioré la sécurité des systèmes d'exploitation, ce qui est probablement dû au fait que les éditeurs de systèmes d'exploitation ont été obligés de régler les problèmes de leurs logiciels. Comme dans le cas des logiciels libres le code source est à la disposition de tous, (SUSE LINUX fournit toutes les sources disponibles), quelqu'un qui découvre une brèche et le code exploit correspondant peut aussitôt faire une proposition de correctif pour le problème en question.

DoS — déni de service (Denial of Service)

Le but de ce type d'attaques est d'interrompre un programme d'un serveur (voire le système tout entier). Cela peut être provoqué par différentes méthodes : en provoquant une surcharge du serveur, en l'occupant en lui envoyant des paquets dont le contenu n'a pas de signification ou en exploitant un débordement de tampon distant. L'objectif d'un déni de service peut souvent tout simplement être que le service ne soit plus disponible. L'absence d'un service peut toutefois avoir d'autres conséquences : les communications peuvent devenir vulnérables à des attaques de *l'homme au milieu* (reniflage de paquets, détournement de connexion TCP, usurpation) et corruption de DNS.

L'homme au milieu : reniflage de paquets, détournement de connexion TCP, usurpation

De manière générale, une attaque distante réalisée par un attaquant qui a pris une position entre deux partenaires de communication s'appelle une attaque de

l'homme au milieu (man in the middle). Les attaques de l'homme au milieu présentent pratiquement comme point commun le fait que la victime ne se doute généralement de rien. Il existe plusieurs variantes. Par exemple, l'attaquant peut prendre la main sur la requête de connexion et la diriger lui-même vers la machine cible. La victime a donc sans le savoir établi une connexion avec le mauvais ordinateur parce que ce dernier s'identifie comme étant la cible légitime.

L'attaque de l'homme au milieu la plus simple est le *reniflage de paquets* (sniffing). L'attaquant épie "simplement" le trafic réseau. Dans une attaque plus complexe, "l'homme au milieu" peut essayer de prendre la main sur une connexion déjà établie (détournement, en anglais hijacking). L'attaquant doit, pour ce faire, analyser pendant un moment les paquets qui lui sont adressés pour pouvoir pronostiquer les numéros de séquence TCP corrects de la connexion. Quand il prend ensuite le rôle de la cible de la connexion, les victimes s'en aperçoivent car ils reçoivent un message d'erreur annonçant que la connexion a été interrompue en raison d'une défaillance.

L'attaquant peut tout particulièrement tirer profit de cette technique car il existe des protocoles non protégés contre le détournement par le chiffrement pour lesquels une authentification ne se produit qu'au début de la connexion.

On parle d'*usurpation* lors d'une attaque avec modification des paquets pour qu'ils contiennent des données sources contrefaites, généralement l'adresse IP. La plupart des variantes d'attaques actives impliquent l'envoi de paquets falsifiés ce qui sous Linux ne peut être effectué que par le super-utilisateur (`root`).

La plupart des possibilités d'attaques sont souvent combinées avec un déni de service. Si l'attaquant a une possibilité de séparer un ordinateur brusquement du réseau, même si ce n'est que pour une courte période, cela lui rend une attaque active plus facile parce que l'hôte ne pourra pas perturber l'attaque pendant un certain temps.

Corruption de DNS (DNS poisoning)

L'attaquant essaie de corrompre le cache d'un serveur DNS avec des paquets de réponse DNS falsifiés pour qu'il transmette certaines données à une victime demandant des informations à ce serveur. Pour passer ce type de fausses informations de manière crédible à un serveur DNS, l'attaquant doit normalement obtenir quelques paquets du serveur et les analyser. Comme de nombreux serveurs ont établi un rapport de confiance vis-à-vis des autres ordinateurs basé sur leur adresse IP ou leur nom d'ordinateur, une telle attaque peut très rapidement porter ses fruits, même si les précautions nécessaires ont été prises. La condition

essentielle est une bonne connaissance des relations de confiance entre les ordinateurs. Du point de vue de l'attaquant, il est la plupart du temps inévitable de programmer précisément dans le temps un déni de service contre un serveur DNS dont les données doivent être falsifiées. Pour y remédier, il convient à nouveau d'utiliser une connexion chiffrée avec une technique cryptographique capable de vérifier l'identité de la cible de la connexion.

Vers

On fait souvent l'amalgame entre les vers et les virus. Il existe cependant une différence sensible entre les deux : un ver n'a nullement besoin d'infecter un programme hôte et il est conçu pour se propager le plus rapidement possible sur le réseau. Les vers les plus connus comme Ramen, Lion ou Adore utilisent les brèches de sécurité de programmes serveur tels que bind8 ou lprNG. Il est relativement facile de se protéger contre les vers, car entre le moment de la découverte des brèches utilisées et le moment de la naissance du vers, il s'écoule généralement quelques jours qui laissent suffisamment de temps pour développer des paquetages de mise à jour ; en partant du principe, naturellement, que l'administrateur applique aussi les mises à jour de sécurité à son système.

34.4.2 Conseils et astuces pour la sécurité

Pour traiter le domaine de la sécurité de manière efficace, il est nécessaire de bien suivre les développements en la matière et de connaître tout ce qui concerne les derniers problèmes de sécurité. Une très bonne méthode de protection contre les erreurs de tous types consiste à appliquer le plus rapidement possible les paquetages de mise à jour signalés lors d'une annonce de sécurité. Les annonces de sécurité de SUSE sont diffusées par liste de diffusion à laquelle vous pouvez vous inscrire à l'adresse suivante : `http://www.novell.com/linux/security/securitysupport.html`. La liste `suse-security-announce@suse.de` est la meilleure source d'informations récentes sur les paquetages de mise à jour fournis par l'équipe de sécurité.

La liste de diffusion `suse-security@suse.de` est un forum de discussion instructif en ce qui concerne le domaine de la sécurité. Vous pouvez vous y inscrire à la même adresse que donnée ci-dessus pour `suse-security-announce@suse.de`.

L'une des listes de diffusion les plus connues au monde en terme de sécurité est la liste `bugtraq@securityfocus.com`. Nous vous recommandons la lecture

attentive de cette liste qui reçoit en moyenne 15 à 20 nouveaux messages chaque jour. Pour plus d'informations, consultez : `http://www.securityfocus.com`.

Voici quelques règles de base à connaître :

- Évitez de travailler en tant qu'utilisateur `root`, et respectez le principe d'utiliser des privilèges minimaux pour effectuer une tâche. Cela permet de réduire les risques d'œuf de coucou ou d'infection par un virus et, de surcroît, les erreurs de votre part.
- Utilisez, dans la mesure du possible, toujours des connexions chiffrées pour effectuer des tâches à distance. `ssh` (secure shell) est le standard pour ce genre de tâches, évitez `telnet`, `ftp`, `rsh` et `rlogin`.
- N'utilisez aucune méthode d'authentification qui serait uniquement fondée sur une adresse IP.
- Tenez vos paquetages réseau les plus importants toujours à jour et abonnez-vous aux listes de diffusion pour recevoir les annonces de ces différents logiciels (bind, sendmail, ssh, etc.). Cela s'applique également aux logiciels qui ne concernent que la sécurité locale.
- Optimisez les droits d'accès aux fichiers critiques en terme de sécurité dans le système en adaptant le fichier `/etc/permissions` en fonction de vos besoins. Un programme setuid qui n'a plus de bit setuid peut certes ne plus remplir sa fonction correctement mais ne représente, en règle générale, aucun problème de sécurité. Vous pouvez utiliser le même processus pour les fichiers et les répertoires pour lesquels tout utilisateur possède les droits d'écriture.
- Désactivez les services réseau dont vous n'avez pas absolument besoin sur votre serveur. Cela permet de rendre votre système plus sûr et cela évite que vos utilisateurs ne s'habituent à un service que vous n'avez jamais activé à dessein (problème d'héritage). Utilisez le programme netstat pour identifier les ports ouverts (ceux dont l'état est LISTEN). Vous disposez des options `netstat -ap` ou `netstat -anp`. L'option `-p` vous permet de voir immédiatement quel processus occupe quel port et sous quel nom.
  Comparez les résultats que vous obtenez avec une analyse complète des ports de votre ordinateur de l'extérieur. Le programme nmap est particulièrement adapté à cet effet. Il interroge chacun des ports et peut, à l'aide de la réponse de votre ordinateur, tirer des conclusions au sujet d'un service en attente derrière le port correspondant. Ne procédez jamais à l'analyse d'un ordinateur sans en avoir averti directement l'administrateur car ce dernier pourrait l'interpréter comme un acte agressif. N'oubliez pas que vous devez non seulement analyser les ports TCP, mais également les ports UDP (options `-sS` et `-sU`).
- Utilisez `tripwire` présent dans la distribution SUSE LINUX pour vérifier, de manière fiable, l'intégrité des fichiers dans votre système et chiffrer la base de

données pour la protéger contre toute manipulation. Vous devez, en outre, toujours effectuer une sauvegarde de cette base de données que vous conserverez en dehors de la machine, sur un support de données indépendant non connecté par l'intermédiaire d'un ordinateur au réseau.

- Faites toujours attention lorsque vous installez des logiciels inconnus. On a déjà vu des cas où l'attaquant avait intégré un cheval de Troie dans l'archive tar d'un logiciel de sécurité. Cela a heureusement rapidement été détecté. Si vous installez un paquetage binaire, vous devez être sûr de sa provenance.
  Les paquetages RPM SUSE livrés sont signés avec une signature gpg. La clé que nous utilisons pour le chiffrement est :
  ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>
  Empreinte de la clé = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA
  La commande `rpm --checksig paquetage.rpm` indique si la somme de contrôle et la signature du paquetage non installé correspondent. Vous trouverez la clé sur le premier CD ou DVD de SUSE LINUX et sur les principaux serveurs de clés du monde.
- Vérifiez régulièrement la sauvegarde de vos données et de votre système. Sans connaissance fiable de la fonction de sauvegarde, une sauvegarde n'a aucune valeur.
- Surveillez vos fichiers journaux. Si vous le pouvez, écrivez un petit script qui recherche dans vos fichiers journaux les éléments inhabituels. Cette tâche n'est vraiment pas triviale car vous êtes le seul à savoir ce qui est habituel ou non.
- Utilisez `tcp_wrapper` pour limiter l'accès aux différents services de votre ordinateur aux adresses IP auxquelles un accès à des services donnés a été accordé. Vous trouverez des informations plus précises au sujet de `tcp_wrapper` dans les pages de manuel de tcpd et `hosts_access` (`man 8 tcpd`, `man hosts_access`).
- Vous pouvez aussi utiliser comme protection supplémentaire, outre tcpd (tcp_wrapper), le pare-feu SuSEfirewall.
- N'ayez pas peur d'être redondant quand il s'agit de sécurité : un message qui s'affiche deux fois est préférable à un que vous ne verriez jamais.

34.4.3 Publication centralisée des nouveaux problèmes de sécurité

Lorsque vous découvrez un problème de sécurité (vérifiez tout d'abord les paquetages de mise à jour disponibles), vous pouvez alors vous adresser en toute confiance à l'adresse électronique suivante : `security@suse.de`. N'oubliez pas de joindre une description précise du problème ainsi que le numéro de version

du paquetage concerné. Nous ferons tout notre possible pour vous répondre le plus rapidement possible. Nous vous recommandons de chiffrer votre message avec pgp. Notre clé pgp est :

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>
Empreinte de la clé = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

Vous pouvez aussi télécharger cette clé à l'adresse suivante : `http://www.novell.com/linux/security/securitysupport.html`.

Listes de contrôle d'accès sous Linux

Ce chapitre présente un bref résumé de l'arrière-plan et des fonctions des ACL POSIX (listes de contrôle d'accès) concernant les systèmes de fichiers Linux. Les ACL peuvent être utilisées à titre d'extension du principe traditionnel de droits d'accès aux objets systèmes de fichiers. Grâce aux ACL, il est possible de définir les droits d'accès avec plus de souplesse que le principe traditionnel de droits d'accès ne le permet.

L’expression *ACL POSIX* suggère qu’il s’agit d’un vrai standard POSIX (*Portable Operating System Interface*, interface de système d’exploitation portable). Pour différentes raisons, les projets de standards respectifs POSIX 1003.1e et POSIX 1003.2c ont été abandonnés. Néanmoins, les ACL telles qu’on les trouve sur de nombreux systèmes appartenant à la famille UNIX sont basés sur ces documents et la mise en œuvre des ACL des systèmes de fichiers comme décrit dans ce chapitre suit ces deux standards également. Vous pouvez les consulter à l’adresse `http://wt.xpilot.org/publications/posix.1e/`.

35.1 Avantages des ACL

Traditionnellement, trois ensembles de droits d’accès sont définis pour chaque objet fichier sur un système Linux. Ils incluent les droits de lecture (`r`), d’écriture (`w`) et d’exécution (`x`) pour chacun des trois types d’utilisateurs—le propriétaire du fichier, le groupe et les autres utilisateurs. En outre, il est possible de définir le bit *set user id*, *set group id* et *sticky*. Dans la pratique courante, ce principe simplifié suffit amplement. Cependant, pour des scénarios plus complexes ou des applications plus avancées, les administrateurs système devaient autrefois avoir recours à un certain nombre d’astuces pour contourner les limites du principe traditionnel de droits d’accès.

Les ACL peuvent être utilisées dans les situations qui requièrent une extension du principe traditionnel des droits d’accès aux fichiers. Elles permettent d’attribuer des droits à des utilisateurs individuels ou à des groupes, même si ces derniers ne correspondent pas au propriétaire originel ou au groupe propriétaire d’un fichier. Les listes de contrôle d’accès sont une fonctionnalité du noyau Linux et sont actuellement prises en charge par ReiserFS, Ext2, Ext3, JFS et XFS. Grâce aux ACL, des scénarios complexes sont réalisables sans avoir à mettre en œuvre des modèles de droits d’accès complexes au niveau des applications.

Les avantages des ACL ressortent de façon évidente dans une situation comme le remplacement d’un serveur Windows par un serveur Linux. Certaines des stations de travail connectées peuvent continuer à tourner sous Windows, même après la migration. Le système Linux propose des services de fichiers et d’impression aux clients Windows grâce à Samba. Étant donné que Samba prend en charge les listes de contrôle d’accès, les droits d’accès utilisateur peuvent être configurés à la fois sur le serveur Linux et sous Windows via une interface graphique (uniquement sous Windows NT et les versions ultérieures). Avec winbindd, il est même possible d’affecter des droits d’accès à des utilisateurs qui n’existent que dans le domaine Windows, sans aucun compte sur le serveur Linux.

35.2 Définitions

Classe d'utilisateurs Le principe conventionnel de droits d'accès POSIX utilise trois *classes* d'utilisateurs pour affecter des droits dans le système de fichiers : le propriétaire, le groupe propriétaire et les autres utilisateurs. Trois bits de droits d'accès peuvent être définis pour chaque classe d'utilisateur, donnant l'accès en lecture (`r`), l'accès en écriture (`w`) et l'accès en exécution (`x`).

ACL d'accès Les droits d'accès, pour les utilisateurs et les groupes, pour tous les types d'objets système de fichiers (fichiers et répertoires) sont déterminés au moyen des ACL d'accès.

ACL par défaut Les ACL par défaut ne peuvent s'appliquer qu'à des répertoires. Elles déterminent les droits d'accès dont un objet système de fichiers hérite de son répertoire parent lors de sa création.

Élément d'ACL Chaque ACL se compose d'un ensemble d'éléments d'ACL. Un élément d'ACL contient un type (voir le tableau tableau 35.1 page suivante), un qualificateur pour l'utilisateur ou le groupe auquel l'élément fait référence, ainsi qu'un ensemble de droits d'accès. Pour certains types d'éléments, le qualificateur pour le groupe ou les utilisateurs est indéfini.

35.3 Gestion des ACL

tableau 35.1 page suivante résume les six types possibles d'éléments d'ACL, dont chacun définit des droits d'accès pour un utilisateur ou un groupe d'utilisateurs. L'élément *owner* (propriétaire)définit les droits d'accès de l'utilisateur propriétaire du fichier ou du répertoire. L'élément *owning group* (groupe propriétaire) définit les droits d'accès du groupe propriétaire du fichier. Le super-utilisateur peut changer le propriétaire ou le groupe propriétaire avec `chown` ou `chgrp`, auquel cas les éléments propriétaire et groupe propriétaire font référence au nouveau propriétaire et groupe propriétaire. Chaque élément *named user* (utilisateur nommé) définit les droits d'accès de l'utilisateur spécifié dans le champ qualificateur de l'élément, qui se trouve dans le champ du milieu sous la forme du texte présenté dans tableau 35.1 page suivante. Chaque élément *named group* définit les droits d'accès du groupe spécifié dans le champ qualificateur de l'élément. Seuls les éléments utilisateur nommé et groupe nommé ont un champ qualificateur qui n'est pas vide. L'élément *other* (autre) définit les droits d'accès de tous les utilisateurs.

L'élément *mask* limite en outre les droits d'accès accordés par les éléments *named user*, *named group* et *owning group* en définissant lesquels parmi les droits d'accès dans ces éléments sont effectifs et lesquels sont masqués. Si des droits existent dans un des éléments mentionnés ainsi que dans le masque, ils sont effectifs. Les droits contenus uniquement dans le masque ou uniquement dans l'élément lui-même ne sont pas effectifs—cela signifie que les droits d'accès ne sont pas accordés. Tous les droits définis dans les éléments *owner* et *owning group* sont toujours effectifs. L'exemple de tableau 35.2 page ci-contre montre ce mécanisme.

Il y a deux classes de base d'ACL : une ACL *minimale* ne contient que les éléments concernant les types *owner*, *owning group* et *other*, ce qui correspond aux bits conventionnels de droits d'accès pour les fichiers et les répertoires. Une ACL *étendue* va au delà de ce principe. Elle doit contenir un élément *mask* et peut inclure plusieurs éléments des types *named user* et *named group*.

TAB. *35.1:* *Types d'éléments d'ACL*

Type	Forme du texte
owner	`user::rwx`
named user	`user:name:rwx`
owning group	`group::rwx`
named group	`group:name:rwx`
mask	`mask::rwx`
other	`other::rwx`

TAB. 35.2: *Masquage de droits d'accès*

Type d'élément	Forme du texte	Droits d'accès
named user	`user:geeko:r-x`	`r-x`
mask	`mask::rw-`	`rw-`
	Droits d'accès effectifs :	`r--`

35.3.1 Éléments d'ACL et bits de droits d'accès du mode fichier

figure 35.1 de la présente page et la figure figure 35.2 page suivante illustrent les deux cas d'une ACL minimale et d'une ACL étendue. Les figures sont structurées en trois blocs—le bloc de gauche présente les spécifications de type des éléments d'ACL, celui du milieu un exemple d'ACL et celui de droite les bits de droits d'accès respectifs conformément au principe conventionnel de droits d'accès, par exemple, comme `ls -l` le montre également. Dans les deux cas, les droits d'accès *owner class* sont mis en correspondance avec l'élément d'ACL *owner*. Les droits d'accès *other class* sont mis en correspondance avec l'élément d'ACL respectif. Cependant, la mise en correspondance des droits d'accès *group class* est différent dans les deux cas.

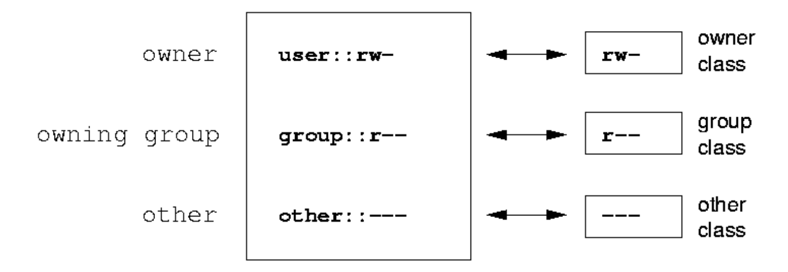


FIG. 35.1: *ACL minimale~: éléments d'ACL comparés aux bits de droits d'accès*

Dans le cas d'une ACL minimale — sans élément *mask* — les droits d'accès *group class* sont mis en correspondance avec l'élément d'ACL *owning group*. Ce comportement est illustré dans figure 35.1 page précédente. Dans le cas d'une ACL étendue — avec *mask* — les droits d'accès *group class* sont mis en correspondance avec l'élément *mask*. Ce comportement est illustré dans figure 35.2 de la présente page.

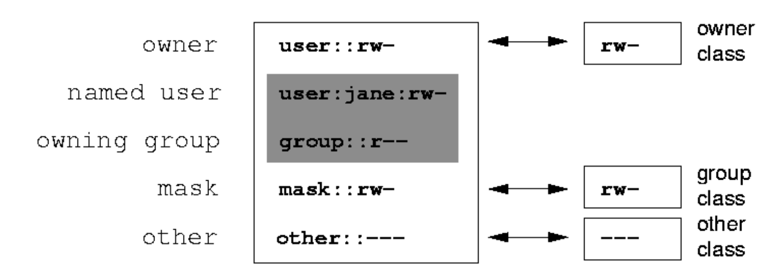


FIG. 35.2: *ACL étendue~: éléments d'ACL comparés aux bits de droits d'accès*

Cette approche de mise en correspondance assure une interaction harmonieuse des applications, qu'elles disposent ou non de la prise en charge des ACL. Les droits d'accès qui ont été affectés au moyen des bits de droits d'accès représentent la limite supérieure pour tous les autres "réglages fins" effectués avec une ACL. Les changements apportés aux bits de droits d'accès sont reflétés par l'ACL et vice versa.

35.3.2 Un répertoire avec une ACL d'accès

La gestion des ACL d'accès est expliquée dans l'exemple suivant :

Avant de créer le répertoire, utilisez la commande `umask` pour définir quels droits d'accès doivent être masqués chaque fois qu'un objet fichier est créé. La commande `umask 027` règle les droits par défaut en donnant au propriétaire l'étendue complète des droits d'accès (`0`), en refusant au l'accès en écriture (`2`) et en ne donnant aucun droit du tout aux autres utilisateurs (`7`). La commande `umask` masque véritablement les bits de droits d'accès correspondants ou les désactive. Pour plus de détails, consultez la page de manuel correspondante (`man umask`).

`mkdir monrep` devrait créer le répertoire `monrep` avec les droits d'accès par

défaut, comme défini par `umask`. Faites appel à `ls -dl monrep` pour vérifier si tous les droits ont été affectés correctement. La sortie de cet exemple est :

```
drwxr-x--- ... tux projet3 ... monrep
```

Avec `getfacl monrep`, vérifiez l'état initial de l'ACL. Celle-ci donne des informations comme :

```
# file: monrep
# owner: tux
# group: projet3
user::rwx
group::r-x
other::---
```

La sortie de `getfacl` reflète précisément la mise en correspondance de bits de droits d'accès avec des éléments d'ACL, comme décrit dans section 35.3.1 page 667. Les trois premières lignes de la sortie affichent le nom, le propriétaire et le groupe propriétaire du répertoire. Les trois lignes suivantes contiennent les trois éléments d'ACL *owner*, *owning group* et *other*. En fait, dans le cas de cette ACL minimale, la commande `getfacl` ne produit aucune information que vous n'auriez pu obtenir avec `ls`.

Modifiez l'ACL pour affecter des droits d'accès en lecture, écriture et exécution à un utilisateur supplémentaire `geeko` et à un groupe supplémentaire `mascottes` avec :

```
setfacl -m user:geeko:rwx,group:mascottes:rwx monrep
```

L'option `-m` invite `setfacl` à modifier l'ACL existante. L'argument suivant indique les éléments d'ACL à modifier (les entrées multiples sont séparées par des virgules). La partie finale spécifie le nom du répertoire auquel ces modifications devront s'appliquer. Utilisez la commande `getfacl` pour jeter un coup d'œil à l'ACL obtenue.

```
# file: monrep
# owner: tux
# group: projet3
user::rwx
user:geeko:rwx
group::r-x
group:mascottes:rwx
mask::rwx
other::---
```

En plus des éléments initiés pour l'utilisateur `geeko` et le groupe `mascottes`, un élément *mask* a été généré. Cet élément *mask* est défini automatiquement, de sorte que tous les droits d'accès sont effectifs. `setfacl` adapte automatiquement les éléments *mask* existants aux réglages modifiés, à moins que vous ne désactiviez cette fonctionnalité avec `-n`. *mask* définit les droits d'accès effectifs maximaux pour tous les éléments dans le *group class*. Ceci inclut *named user*, *named group* et *owning group*. Les bits de droit d'accès de *group class* affichés par `ls -dl monrep` correspondent à présent à l'élément `mask`.

```
drwxrwx---+ ... tux projet3 ... monrep
```

La première colonne de la sortie contient maintenant un + additionnel pour indiquer qu'il y a une ACL *étendue* pour cet élément.

Selon la sortie de la commande `ls`, les droits d'accès pour l'élément *mask* comprennent aussi un accès en écriture. Traditionnellement, de tels bits de droits d'accès signifieraient que le *owning group* (ici `projet3`) a aussi un accès en écriture dans le répertoire `monrep`. Cependant, les droits d'accès effectivement effectifs pour le *owning group* correspondent à la partie se chevauchant des droits d'accès définis pour le *owning group* et le *mask*—qui est `r-x` dans notre exemple (voir tableau 35.2 page 667). Dans la mesure où les droits d'accès effectifs du *owning group* de cet exemple sont concernés, rien n'a changé, même après l'ajout des éléments d'ACL.

Modifiez l'élément *mask* avec `setfacl` ou `chmod`. Par exemple, faites appel à `chmod g-w monrep`. `ls -dl monrep` affiche alors :

```
drwxr-x---+ ... tux projet3 ... monrep
```

`getfacl monrep` fournit la sortie suivante :

```
# file: monrep
# owner: tux
# group: projet3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascottes:rwx     # effective: r-x
mask::r-x
other::---
```

Après avoir exécuté la commande `chmod` pour supprimer le droit d'accès en écriture des bits du *group class*, la sortie de la commande `ls` est suffisante pour voir que les bits *mask* doivent avoir changé en conséquence : le droit d'accès en écriture est à nouveau limité au propriétaire de `monrep`. La sortie de la commande `getfacl` le confirme. Cette sortie comporte un commentaire pour tous ces éléments dans lesquels les bits de droits d'accès effectifs ne correspondent pas aux droits d'origine, parce qu'ils ont été filtrés en fonction de l'élément *mask*. Les droits d'accès d'origine peuvent être restaurés à tout moment avec `chmod g+w monrep`.

35.3.3 Un répertoire avec une ACL par défaut

Les répertoires peuvent avoir une ACL par défaut, ce qui est un type spécial d'ACL définissant les droits d'accès dont les objets présents dans le répertoire héritent quand ils sont créés. Une ACL par défaut affecte à la fois les sous-répertoires et les fichiers.

Effets d'une ACL par défaut

Les droits d'accès dans une ACL par défaut se transmettent différemment aux fichiers et aux sous-répertoires :

- Un sous-répertoire hérite de l'ACL par défaut du répertoire parent aussi bien au titre de son ACL par défaut que de son ACL d'accès.
- Un fichier hérite de l'ACL par défaut au titre de son ACL d'accès.

Tous les appels système qui créent des objets système de fichiers utilisent un paramètre `mode` qui définit les droits d'accès pour l'objet système de fichiers nouvellement créé. Si le répertoire parent n'a pas d'ACL par défaut; les bits de droits d'accès, comme définis par le `umask`, sont soustraits des droits d'accès tels qu'ils sont passés par le paramètre `mode`, le résultat étant affecté au nouvel objet. Si une ACL par défaut existe pour le répertoire parent, les bits de droits d'accès affectés au nouvel objet correspondent à la partie se chevauchent des droits d'accès du paramètre `mode` et ceux qui sont définis dans l'ACL par défaut. L'`umask` est négligé dans ce cas.

Application des ACL par défaut

Les trois exemples suivants montrent les principales opérations sur les répertoires et les ACL par défaut :

1. Ajoutez une ACL par défaut au répertoire existant `monrep` avec :

   ```
   setfacl -d -m group:mascottes:r-x monrep
   ```

   L'option `-d` de la commande `setfacl` invite `setfacl` à effectuer les modifications suivantes (option `-m`) dans l'ACL par défaut.
   Observez de plus près le résultat de cette commande :

   ```
   getfacl monrep

   # file: monrep
   # owner: tux
   # group: projet3
   user::rwx
   user:geeko:rwx
   group::r-x
   group:mascottes:rwx
   mask::rwx
   other::---
   default:user::rwx
   default:group::r-x
   default:group:mascottes:r-x
   default:mask::r-x
   default:other::---
   ```

   `getfacl` renvoie à la fois l'ACL d'accès et l'ACL par défaut. L'ACL par défaut es formée par toutes les lignes qui commencent par `default`. Même si vous avez simplement exécuté la commande `setfacl` avec un élément pour le groupe `mascottes` dans l'ACL par défaut, `setfacl` a automatiquement copié tous les autres éléments provenant de l'ACL d'accès pour créer une ACL par défaut valide. Les ACL par défaut n'ont pas d'effet immédiat sur les droits d'accès. Elles entrent en jeu uniquement lors de la création des objets systèmes de fichiers. Ces nouveaux objets n'héritent de droits d'accès que de l'ACL par défaut de leur répertoire parent.
2. Dans l'exemple suivant, utilisez `mkdir` pour créer un sous-répertoire dans `monrep`, qui hérite de son ACL par défaut.

   ```
   mkdir monrep/monsousrep

   getfacl monrep/monsousrep
   ```

```
# file: monrep/monsousrep
# owner: tux
# group: projet3
user::rwx
group::r-x
group:mascottes:r-x
mask::r-x
other::---
default:user::rwx
default:group::r-x
default:group:mascottes:r-x
default:mask::r-x
default:other::---
```

Comme attendu, le sous-répertoire nouvellement créé `monsousrep` dispose des droits provenant de l'ACL par défaut du répertoire parent. L'ACL d'accès de `monsousrep` est un reflet exact de l'ACL par défaut de `monrep`. L'ACL par défaut que ce répertoire transmet à ses objets subordonnés est également le même.

3. Utilisez `touch` pour créer un fichier dans le répertoire `monrep`, par exemple, `touch monrep/monfichier`. `ls -l monrep/monfichier` affiche alors :

```
-rw-r-----+ ... tux projet3 ... monrep/monfichier
```

La sortie de `getfacl monrep/monfichier` est :

```
# file: monrep/monfichier
# owner: tux
# group: projet3
user::rw-
group::r-x          # effective:r--
group:mascottes:r-x # effective:r--
mask::r--
other::---
```

La commande `touch` utilise un `mode` ayant la valeur `0666` lorsque de nouveaux fichiers sont créés, ce qui signifie que les fichiers sont créés avec des droits d'accès en lecture et en écriture pour toutes les classes d'utilisateurs, du moins s'il n'existe pas d'autres restrictions dans `umask` ou dans l'ACL par défaut (voir section Effets d'une ACL par défaut page 671). Concrètement, cela signifie que tous les droits d'accès non contenus dans la valeur

`mode` sont supprimés des éléments d'ACL respectifs. Bien qu'aucun droit d'accès n'ait été suprimé depuis l'élément d'ACL du *group class*, l'élément *mask* a été modifié pour masquer les droits d'accès non réglés dans `mode`.

Cette approche assure l'interaction harmonieuse des applications, telles que les compilateurs, avec les ACL. Vous pouvez créer des fichiers avec des droits d'accès restreints et les marquer par la suite comme étant exécutables. Le mécanisme `mask` garantit que les utilisateurs et les groupes corrects peuvent les exécuter comme souhaité.

35.3.4 L'algorithme de contrôle d'une ACL

Un algorithme de contrôle est appliqué avant d'accorder à n'importe quel processus ou application l'accès à un objet système de fichiers protégé par des ACL. À titre de règle de base, les éléments sont examinés dans l'ordre suivant :*owner*, *named user*, *owning group* et *named group* et *other*. L'accès est géré en conformité avec l'élément qui convient le mieux au processus. Les droits d'accès ne se cumulent pas.

La situation se complique si un processus appartient à plusieurs groupes et pourrait potentiellement convenir à plusieurs éléments *group*. Un élément est sélectionné aléatoirement parmi les éléments appropriés avec les droits d'accès requis. Le fait de savoir lequel des éléments déclenche le résultat final "accès accordé" n'a pas d'importance. De même, si aucun des éléments *group* approprié ne contient les droits d'accès exigés, un élément sélectionné aléatoirement déclenche le résultat final "access denied".

35.4 Prise en charge dans les applications

Les ACL peuvent être utilisées pour mettre en œuvre des scénarios très complexes de droits d'accès qui répondent aux exigences des applications modernes. Le principe traditionnel de droits d'accès et les ACL peuvent se combiner de manière intelligente. Les commandes de base des fichiers (`cp`, `mv`, `ls`, etc.) prennent en charge les ACL, comme le fait Samba.

Malheureusement, de nombreux éditeurs et gestionnaires de fichiers ne bénéficient pas encore de la prise en charge des ACL. Lorsque vous copiez des fichiers avec Konqueror, par exemple, les ACL de ces fichiers sont perdues. Lorsque vous

modifiez des fichiers avec un éditeur, les ACL des fichiers sont parfois conservées, parfois non, en fonction du mode de sauvegarde de l'éditeur employé. Si l'éditeur écrit les modifications dans le fichier d'origine, l'ACL d'accès est conservée. Si l'éditeur enregistre le contenu mis à jour dans un nouveau fichier qui est renommé ultérieurement avec l'ancien nom de fichier, les ACL risquent d'être perdues, à moins que l'éditeur ne prenne en charge les ACL. En dehors de l'archiveur star, il n'y a actuellement aucune application de sauvegarde qui conserve les ACL.

35.5 Pour plus d'informations

Des informations détaillées sur les ACL sont disponibles à l'adresse : `http://acl.bestbits.at/`. Consultez également es pages de manuel consacrées à `getfacl(1)`, `acl(5)` et `setfacl(1)`..

Utilitaires pour la surveillance du système

Dans ce chapitre vous sont présentés plusieurs programmes et mécanismes différents avec lesquels vous pouvez surveiller l'état de votre système. Vous trouverez ensuite la description de quelques utilitaires intéressants pour votre travail au quotidien avec leurs options les plus importantes.

Vous trouverez des exemples de sorties pour les commandes qui vous sont présentées. La première ligne représente la commande elle-même (après un signe dollar en tant qu'invite). Les omissions sont représentées par `[...]` et les longues lignes peuvent être coupées si nécessaire. Les lignes coupées sont indiquées par un backslash (\) :

```
$ command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
output line 98
output line 99
```

Afin de pouvoir mentionner le plus possible d'utilitaires, leur présentation est faite brièvement. Vous trouverez plus d'informations sur chaque commande à leur page de manuel respective. La plupart des commandes comprennent également l'option `--help`, si bien qu'on obtient une brève liste des options possibles.

36.1 Liste des fichiers ouverts : lsof

Afin d'indiquer la liste de tous les fichiers ouverts pour le processus avec l'ID de processus ⟨*PID*⟩, on utilise l'option `-p`. Par exemple, pour indiquer tous les fichiers utilisés par le shell en cours :

```
$ lsof -p $$
COMMAND  PID USER   FD   TYPE DEVICE    SIZE     NODE NAME
zsh     4694   jj  cwd    DIR   0,18     144 25487368 /suse/jj/t (totan:/real-home/jj)
zsh     4694   jj  rtd    DIR    3,2     608        2 /
zsh     4694   jj  txt    REG    3,2  441296    20414 /bin/zsh
zsh     4694   jj  mem    REG    3,2  104484    10882 /lib/ld-2.3.3.so
zsh     4694   jj  mem    REG    3,2   11648    20610 /usr/lib/zsh/4.2.0/zsh/rlimits.so
[...]
zsh     4694   jj  mem    REG    3,2   13647    10891 /lib/libdl.so.2
zsh     4694   jj  mem    REG    3,2   88036    10894 /lib/libnsl.so.1
zsh     4694   jj  mem    REG    3,2  316410   147725 /lib/libncurses.so.5.4
zsh     4694   jj  mem    REG    3,2  170563    10909 /lib/tls/libm.so.6
zsh     4694   jj  mem    REG    3,2 1349081    10908 /lib/tls/libc.so.6
zsh     4694   jj  mem    REG    3,2      56    12410 /usr/lib/locale/de_DE.utf8/LC_TELEPHONE
[...]
zsh     4694   jj  mem    REG    3,2      59    14393 /usr/lib/locale/en_US/LC_NUMERIC
zsh     4694   jj  mem    REG    3,2  178476    14565 /usr/lib/locale/en_US/LC_CTYPE
zsh     4694   jj  mem    REG    3,2   56444    20598 /usr/lib/zsh/4.2.0/zsh/computil.so
zsh     4694   jj   0u    CHR 136,48                50 /dev/pts/48
zsh     4694   jj   1u    CHR 136,48                50 /dev/pts/48
zsh     4694   jj   2u    CHR 136,48                50 /dev/pts/48
zsh     4694   jj  10u    CHR 136,48                50 /dev/pts/48
```

La variable shell spéciale `$$`, ayant comme valeur l'ID de processus du shell, a été utilisée.

Utilisée sans option, la commande `lsof` énumère tous les fichiers ouverts actuellement. Comme il y en a souvent des milliers, il est rarement utile de tous les afficher. Cependant, cette liste de tous les fichiers peut être combinée avec des fonctions de recherche afin de générer des listes utiles comme, par exemple, une liste de tous les périphériques caractère utilisés :

```
$ lsof | grep CHR
sshd       4685    root  mem    CHR    1,5            45833 /dev/zero
sshd       4685    root  mem    CHR    1,5            45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5            45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5            45833 /dev/zero
zsh        4694      jj    0u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    1u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    2u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj   10u   CHR 136,48               50 /dev/pts/48
X          6476    root  mem    CHR    1,1            38042 /dev/mem
lsof      13478      jj    0u   CHR 136,48               50 /dev/pts/48
lsof      13478      jj    2u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    1u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    2u   CHR 136,48               50 /dev/pts/48
```

36.2 Utilisateur qui accède aux fichiers : fuser

Il peut être utile de déterminer quels processus ou utilisateurs accèdent actuellement à certains fichiers. Supposons, par exemple, que vous souhaitiez démonter un système de fichiers monté sous `/mnt`. `umount` renvoie le message "device is busy." La commande `fuser` peut être utilisée pour déterminer quels processus accèdent au périphérique :

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt
                     jj        26597 f....  less
```

Après la fin du processus `less` qui fonctionnait dans un autre terminal, le système de fichiers se laisse démonter.

36.3 Caractéristiques d'un fichier : stat

On utilise la commande `stat` pour afficher les caractéristiques d'un fichier :

```
$ stat xml-doc.txt
  File: ‘xml-doc.txt’
  Size: 632             Blocks: 8          IO Block: 4096   regular file
Device: eh/14d  Inode: 5938009     Links: 1
Access: (0644/-rw-r--r--)  Uid: (11994/      jj)   Gid: (   50/    suse)
Access: 2004-04-27 20:08:58.000000000 +0200
Modify: 2003-06-03 15:29:34.000000000 +0200
Change: 2003-07-23 17:48:27.000000000 +0200
```

Avec l'option `--filesystem`, les caractéristiques du système de fichiers, sur lequel se trouve le fichier indiqué, sont affichées :

```
 $ stat  . --filesystem
  File: "."
    ID: 0        Namelen: 255     Type: ext2/ext3
Blocks: Total: 19347388   Free: 17831731   Available: 16848938   Size: 4096
Inodes: Total: 9830400    Free: 9663967
```

Si vous utilisez le terminal z shell (`zsh`), saisissez `/usr/bin/stat` car ce terminal a un `stat` intégré avec d'autres options et un format de sortie différent :

```
% type stat
stat is a shell builtin
% stat .
device  769
inode   4554808
mode    16877
nlink   12
uid     11994
gid     50
rdev    0
size    4096
atime   1091536882
mtime   1091535740
ctime   1091535740
blksize 4096
blocks  8
link
```

36.4 Périphériques USB : lsusb

La commande `lsusb` répertorie tous les périphériques USB. Avec l'option `-v`, affichez une liste plus détaillée. On peut lire des informations détaillées dans le

répertoire /proc/bus/usb/. Vous trouvez ci-dessous le résultat de lsusb après qu'une clé mémoire USB ait été attachée. Les dernières lignes indiquent la présence d'un nouveau périphérique.

```
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 001: ID 0000:0000
Bus 001 Device 018: ID 0402:5634 ALi Corp.
```

36.5 Informations relatives à un périphérique SCSI : scsiinfo

La commande scsiinfo affiche les informations relatives à un périphérique SCSI. Avec l'option -l, répertoriez tous les périphériques SCSI connus du système (des informations similaires sont obtenues avec la commande lsscsi). Vous trouvez ci-dessous le résultat de scsiinfo -i /dev/sda, qui donne des informations sur le disque dur. L'option -a donne encore plus d'informations.

```
Inquiry command
---------------
Relative Address                   0
Wide bus 32                        0
Wide bus 16                        1
Synchronous neg.                   1
Linked Commands                    1
Command Queueing                   1
SftRe                              0
Device Type                        0
Peripheral Qualifier               0
Removable?                         0
Device Type Modifier               0
ISO Version                        0
ECMA Version                       0
ANSI Version                       3
AENC                               0
TrmIOP                             0
Response Data Format               2
Vendor:                    FUJITSU
```

```
Product:                       MAS3367NP
Revision level:                0104A0K7P43002BE
```

Il existe une liste de défauts comprenant deux tableaux des mauvais blocs d'un disque dur : celui fourni par le fabricant (manufacturer table) et la liste des mauvais blocs qui apparaissent en cours de fonctionnement (grown table). Si le nombre d'entrées dans la liste "grown table" augmente, il est conseillé de remplacer le disque dur.

36.6 Processus : top

Avec la commande `top` qui signifie "table of processes", une liste des processus qui est actualisée toutes les 2 secondes apparaît. On quitte le programme avec la touche (q). Avec l'option `-n 1`, on arrive à terminer le programme après un seul affichage de la liste de processus. Voici un exemple du résultat de la commande `top -n 1` :

```
top - 14:19:53 up 62 days,  3:35, 14 users,  load average: 0.01, 0.02, 0.00
Tasks: 102 total,   7 running,  93 sleeping,   0 stopped,   2 zombie
Cpu(s):   0.3% user,   0.1% system,   0.0% nice,  99.6% idle
Mem:    514736k total,   497232k used,    17504k free,    56024k buffers
Swap:  1794736k total,   104544k used,  1690192k free,   235872k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  Command
 1426 root      15   0  116m  41m  18m S  1.0  8.2  82:30.34 X
20836 jj        15   0   820  820  612 R  1.0  0.2   0:00.03 top
    1 root      15   0   100   96   72 S  0.0  0.0   0:08.43 init
    2 root      15   0     0    0    0 S  0.0  0.0   0:04.96 keventd
    3 root      34  19     0    0    0 S  0.0  0.0   0:00.99 ksoftirqd_CPU0
    4 root      15   0     0    0    0 S  0.0  0.0   0:33.63 kswapd
    5 root      15   0     0    0    0 S  0.0  0.0   0:00.71 bdflush
        [...]
 1362 root      15   0   488  452  404 S  0.0  0.1   0:00.02 nscd
 1363 root      15   0   488  452  404 S  0.0  0.1   0:00.04 nscd
 1377 root      17   0    56    4    4 S  0.0  0.0   0:00.00 mingetty
 1379 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
 1380 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
```

Pendant que `top` est en marche, on arrive, en appuyant sur la touche (f), à un menu dans lequel le format de la sortie peut être modifié de façon importante.

Afin de surveiller les processus d'un utilisateur défini, l'option `-U UID` peut être utilisée. ⟨*UID*⟩ doit être remplacé par l'ID de l'utilisateur. Avec la commande `top -U $(id -u nom d'utilisateur)`, l'UID de l'utilisateur est recherché à l'aide du nom d'utilisateur et ses processus sont affichés.

36.7 Liste de processus : ps

La commande `ps` créé une liste de processsus. Avec l'option `r`, seuls les processus utilisant des ressources sont affichés :

```
$ ps r
  PID TTY      STAT   TIME COMMAND
22163 pts/7    R      0:01 -zsh
 3396 pts/3    R      0:03 emacs new-makedoc.txt
20027 pts/7    R      0:25 emacs xml/common/utilities.xml
20974 pts/7    R      0:01 emacs jj.xml
27454 pts/7    R      0:00 ps r
```

L'option doit effectivement être saisie sans le signe moins. Les mutliples options sont entrées parfois avec, parfois sans signe moins. La page de manuel est susceptible de faire fuire l'utilisateur potentiel, heureusement, la commande `ps --help` propose une brève page d'assistance.

Pour contrôler le nombre de processus `emacs` en marche, utilisez :

```
$ ps x | grep emacs
 1288 ?        S      0:07 emacs
 3396 pts/3    S      0:04 emacs new-makedoc.txt
 3475 ?        S      0:03 emacs .Xresources
20027 pts/7    S      0:40 emacs xml/common/utilities.xml
20974 pts/7    S      0:02 emacs jj.xml

$ pidof emacs
20974 20027 3475 3396 1288
```

Avec l'option `-p`, les processus sont sélectionnés par l'intermédiaire de l'ID de processus :

```
$ ps www -p $(pidof xterm)
  PID TTY      STAT   TIME COMMAND
 9025 ?        S      0:01 xterm -g 100x45+0+200
 9176 ?        S      0:00 xterm -g 100x45+0+200
29854 ?        S      0:21 xterm -g 100x75+20+0 -fn \
  -B&H-LucidaTypewriter-Medium-R-Normal-Sans-12-120-75-75-M-70-iso10646-1
 4378 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
25543 ?        S      0:02 xterm -g 100x45+0+200
22161 ?        R      0:14 xterm -g 100x45+0+200
16832 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
16912 ?        S      0:00 xterm -g 100x45+0+200
17861 ?        S      0:00 xterm -bg DarkSeaGreen1 -g 120x45+40+300
19930 ?        S      0:13 xterm -bg LightCyan
```

```
21686 ?        S      0:04 xterm -g 100x45+0+200 -fn \
lucidasanstypewriter-12
23104 ?        S      0:00 xterm -g 100x45+0+200
26547 ?        S      0:00 xterm -g 100x45+0+200
```

La liste de processus peut également être formatée selon les besoins. L'option `-L` donne une liste de tous les mots-clés. Si vous souhaitez une liste de tous les processus ordonnés selon l'utilisation qu'ils font des ressources, utilisez la commande suivante :

```
$ ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2    0 [ksoftirqd/0]
    3    0 [events/0]
   17    0 [kblockd/0]
[...]
10164 5260 xterm
31110 5300 xterm
17010 5356 xterm
 3896 29292 /usr/X11R6/bin/X -nolisten tcp -br vt7 -auth /var/lib/xdm/authdir/au
```

36.8 Arborescence de processus : pstree

La commande `pstree` délivre une liste de processus sous forme d'arborescence :

```
$ pstree
init-+-atd
     |-3*[automount]
     |-bdflush
     |-cron
  [...]
     |-usb-storage-1
     |-usb-storage-2
     |-10*[xterm---zsh]
     |-xterm---zsh---mutt
     |-2*[xterm---su---zsh]
     |-xterm---zsh---ssh
     |-xterm---zsh---pstree
     |-ypbind---ypbind---2*[ypbind]
     `-zsh---startx---xinit4-+-X
                             `-ctwm-+-xclock
                                    |-xload
                                    `-xosview.bin
```

Avec l'option `-p`, les noms sont complétés par l'ID de processus. Pour afficher aussi les lignes de commande, on utilise l'option `-a` :

```
$ pstree -pa
init,1
  |-atd,1255
[...]
  '-zsh,1404
      '-startx,1407 /usr/X11R6/bin/startx
          '-xinit4,1419 /suse/jj/.xinitrc [...]
              |-X,1426 :0 -auth /suse/jj/.Xauthority
              '-ctwm,1440
                  |-xclock,1449 -d -geometry -0+0 -bg grey
                  |-xload,1450 -scale 2
                  '-xosview.bin,1451 +net -bat +net
```

36.9 Qui fait quoi : w

Avec la commande `w`, vous pouvez savoir qui est connecté au système et ce qu'il fait. Exemple :

```
$ w
 15:17:26 up 62 days,  4:33, 14 users,  load average: 0.00, 0.04, 0.01
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
jj       pts/0     30Mar04  4days  0.50s  0.54s xterm -e su -l
jj       pts/1     23Mar04  5days  0.20s  0.20s -zsh
jj       pts/2     23Mar04  5days  1.28s  1.28s -zsh
jj       pts/3     23Mar04  3:28m  3.21s  0.50s -zsh
[...]
jj       pts/7     07Apr04  0.00s  9.02s  0.01s w
jj       pts/9     25Mar04  3:24m  7.70s  7.38s mutt
[...]
jj       pts/14    12:49   37:34   0.20s  0.13s ssh totan
```

La dernière ligne révèle que l'utilisateur jj a créé une liaison secure shell (`ssh`)vers l'ordinateur `totan`. Si des utilisateurs d'autres systèmes se sont connectés à distance, on peut alors faire afficher, à l'aide de l'option `-f`, à partir de quel ordinateur ils ont créé cette liaison.

36.10 Utilisation de la mémoire : free

L'utilisation de la mémoire vive (RAM) est examinée à l'aide de l'utilitaire `free`. Il indique la mémoire libre et la mémoire occupée (et les zones swap) :

```
$ free
             total       used       free     shared    buffers     cached
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

Avec l'option `-m`, toutes les tailles sont indiquées en mégaoctets :

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

La donnée réellement intéressante se trouve à la ligne suivante :

```
-/+ buffers/cache:        191        311
```

Ici, l'utilisation de la mémoire par les tampons et caches est calculée. Avec l'option `-d délai` , la sortie est renouvelée toutes les ⟨*délai*⟩ secondes : Par exemple, `free -d 1.5` émet toutes les 1,5 secondes les valeurs actuelles.

36.11 Tampon circulaire du noyau : dmesg

Le noyau Linux conserve une certaine quantité de messages dans un tampon circulaire. Ces messages sont publiés à l'aide de la commande `dmesg` :

```
$ dmesg
[...]
sdc : READ CAPACITY failed.
sdc : status = 1, message = 00, host = 0, driver = 08
Info fld=0xa00 (nonstd), Current sd00:00: sense key Not Ready
sdc : block size assumed to be 512 bytes, disk size 1GB.
sdc: test WP failed, assume Write Enabled
 sdc: I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 unable to read partition table
 I/O error: dev 08:20, sector 0
nfs: server totan not responding, still trying
nfs: server totan OK
```

L'avant-dernière ligne indique un problème temporaire du serveur NFS `totan`. Les lignes avant celle-ci sont déclenchées par le branchement d'un flash drive USB. Les événements plus ancienx sont enregistrés dans les fichiers `/var/log/messages` et `/var/log/warn`.

36.12 Systèmes de fichiers et utilisation : mount, df et du

La commande `mount` montre quel système de fichier (périphérique et type) est monté eà quel endroit (point de montage) :

```
$ mount
/dev/hdb2 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/hda1 on /data type ext2 (rw)
shmfs on /dev/shm type shm (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
automount(pid1012) on /suse type autofs \
    (rw,fd=5,pgrp=1012,minproto=2,maxproto=3)
totan:/real-home/jj on /suse/jj type nfs \
    (rw,nosuid,rsize=8192,wsize=8192,hard,intr,nolock,addr=10.10.0.1)
```

L'utilisation caractéristique générale du système de fichiers peut être interrogée avec `df`. L'option `-h` (ou `--human-readable`) rend l'information lisible pour tous :

```
$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdb2             7.4G  5.1G  2.0G  73% /
/dev/hda1              74G  5.8G   65G   9% /data
shmfs                 252M     0  252M   0% /dev/shm
totan:/real-home/jj   350G  324G   27G  93% /suse/jj
```

Il est préférable que les utilisateurs du serveur de fichiers NFS `totan` mettent de l'ordre dans leurs répertoires personnels le plus vite possible. On peut connaître la taille globale de tous les fichiers à l'intérieur d'un répertoire à l'aide de la commande `du`. L'option `-s` empêche la sortie détaillée, `-h` améliore également la lisibilité pour tout un chacun. Avec la commande suivante :

```
$ du -sh ~
361M    /suse/jj
```

on peut estimer la place nécessaire à son propre répertoire personnel.

36.13 Le système de fichiers /proc

Le système de fichiers `/proc` est un pseudo système de fichiers dans lequel le noyau détient des informations importantes sous forme de fichiers virtuels. Par exemple, le type de CPU peut être affiché avec cette commande :

```
$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm) XP 2400+
stepping        : 1
cpu MHz         : 2009.343
cache size      : 256 KB
fdiv_bug        : no
[...]
```

On retrouve l'affectation et l'utilisation des interruptions avec :

```
$ cat /proc/interrupts
           CPU0
  0:  537544462          XT-PIC  timer
  1:     820082          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          2          XT-PIC  rtc
  9:          0          XT-PIC  acpi
 10:      13970          XT-PIC  usb-uhci, usb-uhci
 11:  146467509          XT-PIC  ehci_hcd, usb-uhci, eth0
 12:    8061393          XT-PIC  PS/2 Mouse
 14:    2465743          XT-PIC  ide0
 15:       1355          XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0
```

Voici une liste de certains fichiers importants et des informations qu'ils contiennent :

`/proc/devices` périphériques disponibles

`/proc/modules` modules du noyau chargés

`/proc/cmdline` ligne de commande du noyau

`/proc/meminfo` informations détaillées sur l'utilisation de la mémoire

/proc/config.gz gzip fichier de configuration comprimé du noyau fonctionnant actuellement.

Vous trouverez des informations complémentaires dans le fichier texte : /usr/src/linux/Documentation/filesystems/proc.txt. Des informations sur les processus en cours se trouvent dans les répertoires /proc/ ⟨*NNN*⟩, ⟨*NNN*⟩ étant l'ID de processus (PID) de chaque processus. Sous /proc/self/, chaque processus trouve ses propres caractéristiques :

```
$ ls -l /proc/self
lrwxrwxrwx  1 root root 64 Apr 29 13:52 /proc/self -> 27585

$ ls -l /proc/self/
total 0
dr-xr-xr-x  2 jj suse 0 Apr 29 13:52 attr
-r--------  1 jj suse 0 Apr 29 13:52 auxv
-r--r--r--  1 jj suse 0 Apr 29 13:52 cmdline
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 cwd -> /suse/jj/t
-r--r--r--  1 jj suse 0 Apr 29 13:52 delay
-r--------  1 jj suse 0 Apr 29 13:52 environ
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 exe -> /bin/ls
dr-x------  2 jj suse 0 Apr 29 13:52 fd
-rw-------  1 jj suse 0 Apr 29 13:52 mapped_base
-r--r--r--  1 jj suse 0 Apr 29 13:52 maps
-rw-------  1 jj suse 0 Apr 29 13:52 mem
-r--r--r--  1 jj suse 0 Apr 29 13:52 mounts
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 root -> /
-r--r--r--  1 jj suse 0 Apr 29 13:52 stat
-r--r--r--  1 jj suse 0 Apr 29 13:52 statm
-r--r--r--  1 jj suse 0 Apr 29 13:52 status
dr-xr-xr-x  3 jj suse 0 Apr 29 13:52 task
-r--r--r--  1 jj suse 0 Apr 29 13:52 wchan
```

Dans le fichier maps, on trouve l'attribution des adresses des exécutables et des bibliothèques :

```
$ cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:02 22890      /bin/cat
0804c000-0804d000 rw-p 00003000 03:02 22890      /bin/cat
0804d000-0806e000 rwxp 0804d000 00:00 0
40000000-40016000 r-xp 00000000 03:02 10882      /lib/ld-2.3.3.so
40016000-40017000 rw-p 00015000 03:02 10882      /lib/ld-2.3.3.so
40017000-40018000 rw-p 40017000 00:00 0
4002b000-40135000 r-xp 00000000 03:02 10908      /lib/tls/libc.so.6
40135000-4013d000 rw-p 0010a000 03:02 10908      /lib/tls/libc.so.6
4013d000-40141000 rw-p 4013d000 00:00 0
bfffe000-c0000000 rw-p bfffe000 00:00 0
ffffe000-fffff000 ---p 00000000 00:00 0
```

36.14 vmstat, iostat et mpstat

L'utilitaire `vmstat` fait état des statistiques de la mémoire virtuelle. Il lit les fichiers `/proc/meminfo`, `/proc/stat` et `/proc/*/stat`. Il est utile pour identifier les ralentissements des performances du système.

La commande `iostat` fait état des statistiques du processeur et des entrées et sorties pour les périphériques et partitions. Les informations affichées sont extraites des fichiers `/proc/stat` et `/proc/partitions`. La sortie peut être utilisée pour mieux équilibrer la charge d'entrée et de sortie entre les disques durs. La commande `mpstat` fait état des statistiques liées au processeur.

36.15 procinfo

Les informations importantes provenant du système de fichiers `/proc` sont récapitulées à l'aide de la commande `procinfo` :

```
$ procinfo
Linux 2.6.4-54.5-default (geeko@buildhost) (gcc 3.3.3 ) #1 1CPU [roth.suse.de]


Memory:      Total        Used        Free      Shared     Buffers
Mem:        516696      513200        3496           0       43284
Swap:       530136        1352      528784

Bootup: Wed Jul  7 14:29:08 2004    Load average: 0.07 0.04 0.01 1/126 5302

user  :       2:42:28.08   1.3%  page in :        0
nice  :       0:31:57.13   0.2%  page out:        0
system:       0:38:32.23   0.3%  swap in :        0
idle  :   3d 19:26:05.93  97.7%  swap out:        0
uptime:   4d  0:22:25.84         context :207939498

irq  0: 776561217 timer                 irq  8:         2 rtc
irq  1:    276048 i8042                 irq  9:     24300 VIA8233
irq  2:         0 cascade [4]           irq 11:  38610118 acpi, eth0, uhci_hcd
irq  3:         3                       irq 12:   3435071 i8042
irq  4:         3                       irq 14:   2236471 ide0
irq  6:         2                       irq 15:       251 ide1
```

Pour voir "toutes" les informations, utilisez l'option `-a`. Avec l'option `-nN` , les informations seront rafraichies toutes les ⟨*N*⟩ secondes. Dans ce cas, vous devez quitter le programme avec la touche [q].

Par défaut, les valeurs cumulées sont affichées. On indique les valeurs différentielles avec l'option `-d`. `procinfo -dn5` indique les valeurs changées durant les cinq dernières secondes :

```
Memory:      Total        Used        Free      Shared     Buffers      Cached
Mem:             0           2          -2           0           0           0
Swap:            0           0           0

Bootup: Wed Feb 25 09:44:17 2004    Load average: 0.00 0.00 0.00 1/106 31902

user  :       0:00:00.02   0.4%  page in :        0  disk 1:        0r       0w
nice  :       0:00:00.00   0.0%  page out:        0  disk 2:        0r       0w
system:       0:00:00.00   0.0%  swap in :        0  disk 3:        0r       0w
idle  :       0:00:04.99  99.6%  swap out:        0  disk 4:        0r       0w
uptime:  64d  3:59:12.62         context :     1087

irq  0:       501 timer                 irq 10:         0 usb-uhci, usb-uhci
irq  1:         1 keyboard              irq 11:        32 ehci_hcd, usb-uhci,
irq  2:         0 cascade [4]           irq 12:       132 PS/2 Mouse
irq  6:         0                       irq 14:         0 ide0
irq  8:         0 rtc                   irq 15:         0 ide1
irq  9:         0 acpi
```

36.16 Ressources PCI : lspci

La commande `lspci` énumère les ressources PCI :

```
$ lspci
00:00.0 Host bridge: VIA Technologies, Inc. \
    VT8366/A/7 [Apollo KT266/A/333]
00:01.0 PCI bridge: VIA Technologies, Inc. \
    VT8366/A/7 [Apollo KT266/A/333 AGP]
00:0b.0 Ethernet controller: Digital Equipment Corporation \
    DECchip 21140 [FasterNet] (rev 22)
00:10.0 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.1 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.2 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.3 USB Controller: VIA Technologies, Inc. USB 2.0 (rev 82)
00:11.0 ISA bridge: VIA Technologies, Inc. VT8235 ISA Bridge
00:11.1 IDE interface: VIA Technologies, Inc. VT82C586/B/686A/B \
    PIPC Bus Master IDE (rev 06)
00:11.5 Multimedia audio controller: VIA Technologies, Inc. \
    VT8233 AC97 Audio Controller (rev 50)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. \
    MGA G550 AGP (rev 01)
```

Avec l'option `-v`, l'affichage est plus détaillé :

```
$ lspci -v
[...]
01:00.0 \
 VGA compatible controller: Matrox Graphics, Inc. MGA G550 AGP (rev 01) \
    (prog-if 00 [VGA])
 Subsystem: Matrox Graphics, Inc. Millennium G550 Dual Head DDR 32Mb
 Flags: bus master, medium devsel, latency 32, IRQ 10
```

```
 Memory at d8000000 (32-bit, prefetchable) [size=32M]
 Memory at da000000 (32-bit, non-prefetchable) [size=16K]
 Memory at db000000 (32-bit, non-prefetchable) [size=8M]
 Expansion ROM at <unassigned> [disabled] [size=128K]
 Capabilities: <available only to root>
```

La résolution des noms des périphériques est effectuée avec le fichier `/usr/share/pci.ids`. Les ID PCI n'apparaissant pas dans ce fichier sont indiquées comme "Unknown device".

On reçoit avec `-vv` toutes les informations pouvant être appelées par le programme. Les valeurs purement numériques sont indiquées à l'aide de l'option `-n`.

36.17 Appels système d'un processus : strace

On peut suivre tous les appels système d'un processus en cours à l'aide de l'utilitaire `strace`. On entre la commande comme à l'habitude, complétée d'un `strace` en début de ligne :

```
$ strace -e open ls

execve("/bin/ls", ["ls"], [/* 88 vars */]) = 0
uname({sys="Linux", node="edison", ...}) = 0
brk(0)                                  = 0x805b000
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
          = 0x40017000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=76333, ...}) = 0
old_mmap(NULL, 76333, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40018000
[...]
ioctl(1, SNDCTL_TMR_TIMEBASE or TCGETS, {B38400 opost isig icanon echo ...}) = 0
ioctl(1, TIOCGWINSZ, {ws_row=53, ws_col=110, ws_xpixel=897, ws_ypixel=693}) = 0
open(".", O_RDONLY|O_NONBLOCK|O_LARGEFILE|O_DIRECTORY) = 3
fstat64(3, {st_mode=S_IFDIR|0755, st_size=144, ...}) = 0
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
getdents64(3, /* 5 entries */, 4096)    = 160
getdents64(3, /* 0 entries */, 4096)    = 0
close(3)                                = 0
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 48), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
          = 0x40018000
write(1, "ltrace-ls.txt  myfile.txt  strac"..., 41) = 41
munmap(0x40018000, 4096)                = 0
exit_group(0)                           = ?
```

Par exemple, pour suivre toutes les tentatives d'ouverture d'un fichier, on procède comme suit :

```
$ strace -e open ls myfile.txt

open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
open("/lib/tls/librt.so.1", O_RDONLY)   = 3
open("/lib/libacl.so.1", O_RDONLY)      = 3
open("/lib/libselinux.so.1", O_RDONLY)  = 3
open("/lib/tls/libc.so.6", O_RDONLY)    = 3
open("/lib/tls/libpthread.so.0", O_RDONLY) = 3
open("/lib/libattr.so.1", O_RDONLY)     = 3
open("/proc/mounts", O_RDONLY)          = 3
[...]
open("/proc/filesystems", O_RDONLY)     = 3
open("/proc/self/attr/current", O_RDONLY) = 4
```

Pour suivre également tous les processus enfants, on utilise l'option `-f`. On peut parfaitement contrôler le comportement et le format de sortie de strace, voir à ce sujet `man strace`.

36.18 Appels bibliothèque d'un processus : ltrace

Les appels bibliothèque d'un processus peuvent être suivis à l'aide de la commande `ltrace`. Le principe d'utilisation est le même que pour `strace`. Avec l'option `-c`, le nombre et la durée des appels bibliothèque effectués est affiché :

```
$ ltrace -c find /usr/share/doc
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 86.27    1.071814          30     35327           write
 10.15    0.126092          38      3297           getdents64
  2.33    0.028931           3     10208           lstat64
  0.55    0.006861           2      3122         1 chdir
  0.39    0.004890           3      1567         2 open
[...]
  0.00    0.000003           3         1           uname
  0.00    0.000001           1         1           time
------ ----------- ----------- --------- --------- ----------------
100.00    1.242403                 58269         3 total
```

36.19 Spécifier la bibliothèque nécessaire : ldd

A l'aide de la commande `ldd` on sait quelles bibliothèques seraient chargées par le programme dynamique exécutable donné en argument :

```
$ ldd /bin/ls
linux-gate.so.1 =>  (0xffffe000)
librt.so.1 => /lib/tls/librt.so.1 (0x4002b000)
libacl.so.1 => /lib/libacl.so.1 (0x40033000)
libselinux.so.1 => /lib/libselinux.so.1 (0x40039000)
libc.so.6 => /lib/tls/libc.so.6 (0x40048000)
libpthread.so.0 => /lib/tls/libpthread.so.0 (0x4015d000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
libattr.so.1 => /lib/libattr.so.1 (0x4016d000)
```

Les exécutables statiques n'ont besoin d'aucune bibliothèque dynamique :

```
$ ldd /bin/sash
        not a dynamic executable
$ file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
for GNU/Linux 2.2.5, statically linked, stripped
```

36.20 Informations sur les fichiers binaires ELF

Le contenu des fichiers binaires peut être lu à l'aide de l'utilitaire `readelf`. Ceci fonctionne aussi avec les fichiers ELF qui sont conçus pour d'autres architectures :

```
$ readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
```

```
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8049b40
  Start of program headers:          52 (bytes into file)
  Start of section headers:          76192 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         9
  Size of section headers:           40 (bytes)
  Number of section headers:         29
  Section header string table index: 26
```

36.21 Communication inter-processus : ipcs

Avec la commande `ipcs`, on reçoit une énumération des ressources IPC utilisées :

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x000027d9 5734403    toms      660        64528      2
0x00000000 5767172    toms      666        37044      2
0x00000000 5799941    toms      666        37044      2

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x000027d9 0          toms      660        1

------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

36.22 Mesure du temps avec time

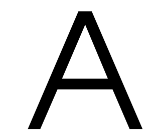
Le besoin en temps des commandes peut être retrouvé grâce au programme d'aide `time`. Cet utilitaire est disponible en deux versions : d'une part intégré au shell et d'autre part en tant que programme (`/usr/bin/time`).

```
$ time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

Cinquième partie

Appendices



Sources d'information et documentations

Une vaste gamme de sources d'information qui s'appliquent à votre système SUSE LINUX existent. Certaines de ces sources sont spécifiques à SUSE, mais beaucoup sont des sources plus générales. Certaines sont déjà disponibles sur votre système ou sur les supports d'installation, et d'autres sont accessible par Internet.

Documentation SUSE

Vous trouverez d'amples informations sur ce sujet dans nos manuels au format HTML ou PDF dans les paquetages RPM `suselinux-userguide_fr` et `suselinux-adminguide_fr`). Dans le cas d'une installation standard, les manuels sont installés dans le répertoire `/usr/share/doc/manual/`. À l'aide du centre d'aide de SUSE, vous avez accès à ces informations.

Le projet de documentation Linux (LDP, Linux Documentation Project)

Le projet de documentation Linux (voir `http://www.tldp.org/`) est une équipe de volontaires qui créent une documentation sur Linux. Le LDP comporte des HOWTO, FAQ et ce qu'on appelle des guides (manuels), tous publiés sous une licence libre.

Les HOWTO ("Comment faire ?") sont des modes d'emploi pas à pas et s'adressent à l'utilisateur final, aux administrateurs de système ou aux programmeurs. Par exemple, l'installation d'un serveur DHCP ainsi que ce à quoi il faut veiller est décrit dans un HOWTO, mais pas la façon d'installer Linux en tant que tel. En règle générale, de telles documentations sont assez générales afin de pouvoir être utilisées pour chaque distribution. Le paquetage `howto` comporte des "Comment faire..." au format ASCII. Les utilisateurs préférant HTML installeront `howtoenh`.

Les FAQ (Foires Aux Questions) sont un ensemble de questions et réponses concernant des domaines de problèmes définis, fréquemment posées dans les listes de discussion. Par exemple, "Qu'est-ce que LDAP ?", "Qu'est-ce qu'un RAID ?", etc. Les textes de cette catégorie sont en général très courts.

Les guides sont des manuels qui peuvent traiter un thème de manière beaucoup plus détaillée que les "Comment faire..." et les FAQ. Par exemple la programmation du noyau, l'administration du réseau, entre autres. L'objectif est de transmettre une connaissance solide au lecteur.

Beaucoup de documentations du LDP sont également disponibles en d'autres formats, comme par exemple PDF, des pages HTLML isolées ou multiples, PostScript et sous forme de sources SGML/XML. Il existe également parfois des traductions dans différentes langues.

Pages de manuel et d'information

Une page de manuel (en anglais Manual page) est un texte d'aide sur une commande, un appel système, un format de fichier, entre autres. Habituellement, une page de manuel est subdivisée en différentes sections, comme Nom, Syntaxe, Description, Options, Fichiers, etc.

Pour afficher une page de manuel, saisissez `man ls`. Cette commande affiche le texte d'aide relatif à la commande `ls`. Avec les touches curseur, vous pouvez déplacer la partie visible, avec q vous quittez `man`. Pour imprimer une page de manuel (par exemple, pour la commande `ls`), saisissez une commande telle que `man -Tps | lpr`. Vous trouverez plus d'aide concernant la commande `man` avec l'option `--help` ou la page de manuel de man (`man man`).

Beaucoup de documentations sont également disponibles dans le format Info, par exemple `grep`. On l'appelle avec `info grep`.

Contrairement aux pages de manuel, les pages d'info sont plus détaillées. Elles sont divisées en plusieurs *points* un point représente alors une page pouvant être



lue avec un lecteur de fichiers info, qui fonctionne globalement comme un navigateur web. Pour naviguer dans une page d'info, utilisez les touches Ⓟ (previous, page précédente) et Ⓝ (next, page suivante). Avec Ⓠ, vous quittez `info`. Vous trouverez les informations sur les autres touches dans la documentation relative à `info` (`info info`).

On peut appeler aussi bien les pages de manuel que les pages d'info dans Konqueror en entrant `man:`⟨*Commande*⟩ ou `info:`⟨*Commande*⟩ dans la ligne d'URL.

Standards et spécifications

Si vous avez besoin d'informations sur les standards ou les spécifications, il existe pour cela différentes possibilités d'information :

`www.linuxbase.org` Le Free Standards Group est un organisme indépendant à but non lucratif dont l'objectif est d'assister la diffusion de logiciels libres et de logiciels Open Source. Ceci doit être réalisé grâce à la définition de standards communs aux distributions. La maintenance de plusieurs standards, entre autres le très important LSB (Linux Standard Base), est effectuée sous la direction de cet organisme.

`http://www.w3.org` Le World Wide Web Consortium (W3C) est l'une des organisations de standardisation les plus connues. Il a été créé en octobre 1994 par Tim Berners-Lee et se concentre sur la standardisation de technologies Web. Le W3C encourage la diffusion de spécifications ouvertes, sans licence et indépendantes du fabricant comme par exemple HTML, XHTML et XML. Ces standards du Web sont développés dans un processus à 4 niveaux dans ce qu'on appelle des *Working Groups* (groupes de travail) et sont présentés au public comme des *recommandations W3C* (REC).

`http://www.oasis-open.org` OASIS (Organization for the Advancement of Structured Information Standards) est un consortium international spécialisé dans le développement de standards relatifs à la sécurité sur le Web, le commerce électronique, les transactions commerciales, la logistique et l'interopérabilité entre différents marchés.

`http://www.ietf.org` L'Internet Engineering Task Force (IETF) est une communauté, agissant au niveau international, de chercheurs, designers de réseau, fournisseurs et utilisateurs. Elle se concentre sur le développement de l'architecture internet et le bon fonctionnement d'internet par l'intermédiaire de protocoles.

Chaque standard IETF est publié en tant que RFC (Request for Comments, cf. `http://www.ietf.org/rfc.html`) et est gratuit. Il existe six sortes de RFC : propsed standards, draft standards, Internet standards, experimental protocols, Informational documents et historic standards. Seules les trois premières (proposed, draft, et full) sont des standards IETF au sens strict du terme (cf. également un résumé à ce sujet sous `http://www.ietf.org/rfc/rfc1796.txt`).

`http://www.ieee.org` L'Institute of Electrical and Electronics Engineers (IEEE) est une organisation qui crée les standards dans les domaines de la technologie d'information, des télécommunications, de la médecine et de la santé, du transport, entre autres. Les standards IEEE sont payants.

`http://www.iso.org` Le comité ISO (Internationl Organization for Standards) est le plus grand développeur de standards et gère un réseau d'instituts de standardisation nationaux dans plus de 140 pays. Les standards ISO sont payants.

`http://www.din.de`, `http://www.din.com`
Le Deutsches Institut für Normung (DIN) est une association technico-scientifique déclarée qui fut fondée en 1917. DIN se définit comme "l'institution responsable en Allemagne des travaux de normalisation et le représentant des intérêts allemands dans les organisations de normalisation internationales et européeenne".

L'association est un regroupement de fabricants, consommateurs, artisans, entreprises de prestation de services, scientifiques et autres personnes qui sont intéressés par la création de normes. Les normes sont payantes et peuvent être commandées sur le site de DIN.

Vérification du système de fichiers

Page de manuel de reiserfsck

```
REISERFSCK(8)                                          REISERFSCK(8)

NAME
       reiserfsck - check a Linux Reiserfs file system

SYNOPSIS
       reiserfsck  [  -afprVy ] [ --rebuild-sb | --check | --fix-
       fixable | --rebuild-tree | --clean-attributes  ]  [  -j  |
       --journal device ] [ -z | --adjust-size ] [ -n | --nolog ]
       [ -l | --logfile file ] [ -q | --quiet ] [ -y | --yes ]  [
       -S  |  --scan-whole-partition ] [ --no-journal-available ]
       device

DESCRIPTION
       Reiserfsck searches for a Reiserfs filesystem on a device,
       replays  any  necessary transactions, and either checks or
       repairs the file system.

       device is the special file corresponding to the device  or
              partition  (e.g /dev/hdXX for IDE disk partition or
              /dev/sdXX for SCSI disk partition).

OPTIONS
       --rebuild-sb
```

This option recovers the superblock on a Reiserfs partition. Normally you only need this option if mount reports "read_super_block: can't find a reis erfs file system" and you are sure that a Reiserfs file system is there.

--check
This default action checks file system consistency and reports but does not repair any corruption that it finds. This option may be used on a read-only file system mount.

--fix-fixable
This option recovers certain kinds of corruption that do not require rebuilding the entire file sys tem tree (--rebuild-tree). Normally you only need this option if the --check option reports "corrup tion that can be fixed with --fix-fixable". This includes: zeroing invalid data-block pointers, cor recting st_size and st_blocks for directories, and deleting invalid directory entries.

--rebuild-tree
This option rebuilds the entire file system tree using leaf nodes found on the device. Normally you only need this option if the --check option reports "corruption that can be fixed only during --rebuild-tree". You are strongly encouraged to make a backup copy of the whole partition before attempting the --rebuild-tree option.

--clean-attributes
This option cleans reserved fields of Stat-Data items.

--journal device , -j device
This option supplies the device name of the current file system journal. This option is required when the journal resides on a separate device from the main data device (although it can be avoided with the expert option --no-journal-available).

--adjust-size, -z

```
       This option causes reiserfsck to correct file sizes
       that are larger than the offset of the last discov
       ered byte.  This implies that holes at the end of a
       file will be removed.  File sizes that are  smaller
       than  the  offset  of  the last discovered byte are
       corrected by --fix-fixable.

--logfile file, -l  file
       This option causes reiserfsck to report any corrup
       tion it finds to the specified log file rather than
       stderr.

--nolog, -n
       This option prevents reiserfsck from reporting  any
       kinds of corruption.

--quiet, -q
       This  option prevents reiserfsck from reporting its
       rate of progress.

--yes, -y
       This option inhibits reiserfsck from asking you for
       confirmation  after telling you what it is going to
       do, assuming yes. For safety, it does not work with
       the --rebuild-tree option.

-a, -p These  options are usually passed by fsck -A during
       the automatic checking of those  partitions  listed
       in  /etc/fstab.  These  options cause reiserfsck to
       print some information  about  the  specified  file
       system,  check if error flags in the superblock are
       set and  do  some  light-weight  checks.  If  these
       checks reveal a corruption or the flag indicating a
       (possibly fixable) corruption is found set  in  the
       superblock,  then  reiserfsck  switches to the fix-
       fixable mode. If the flag indicating a  fatal  cor
       ruption  is found set in the superblock, then reis
       erfsck finishes with an error.

-V     This option prints the  reiserfsprogs  version  and
       exit.

-r, -f These options are ignored.
```

EXPERT OPTIONS

DO NOT USE THESE OPTIONS UNLESS YOU KNOW WHAT YOU ARE DOING. WE ARE NOT RESPONSIBLE IF YOU LOSE DATA AS A RESULT OF THESE OPTIONS.

--no-journal-available

This option allows reiserfsck to proceed when the journal device is not available. This option has no effect when the journal is located on the main data device. NOTE: after this operation you must use reiserfstune to specify a new journal device.

--scan-whole-partition, -S

This option causes --rebuild-tree to scan the whole partition, not only used space on the partition.

EXAMPLE OF USING

1. You think something may be wrong with a reiserfs partition on /dev/hda1 or you would just like to perform a periodic disk check.

2. Run reiserfsck --check --logfile check.log /dev/hda1. If reiserfsck --check exits with status 0 it means no errors were discovered.

3. If reiserfsck --check exits with status 1 (and reports about fixable corruptions) it means that you should run reiserfsck --fix-fixable --logfile fixable.log /dev/hda1.

4. If reiserfsck --check exits with status 2 (and reports about fatal corruptions) it means that you need to run reiserfsck --rebuild-tree. If reiserfsck --check fails in some way you should also run reiserfsck --rebuild-tree, but we also encourage you to submit this as a bug report.

5. Before running reiserfsck --rebuild-tree, please make a backup of the whole partition before proceeding. Then run reiserfsck --rebuild-tree --logfile rebuild.log /dev/hda1.

6. If the --rebuild-tree step fails or does not recover what you expected, please submit this as a bug report. Try to provide as much information as possible and we will try

```
       to help solve the problem.

EXIT CODES
       reiserfsck uses the following exit codes:
          0 - No errors.
          1 - File system errors corrected.
          4 - File system fatal errors left uncorrected,
              reiserfsck --rebuild-tree needs to be launched.
          6 - File system fixable errors left uncorrected,
              reiserfsck --fix-fixable needs to be launched.
          8 - Operational error.
          16 - Usage or syntax error.

AUTHOR
       This version of reiserfsck  has  been  written  by  Vitaly
       Fertman <vitaly@namesys.com>.

BUGS
       There  are  likely  to be some bugs. Please report bugs to
       the ReiserFS mail-list <reiserfs-list@namesys.com>.

TODO
       Faster recovering, signal handling,  i/o  error  handling,
       etc.

SEE ALSO
       mkreiserfs(8),  reiserfstune(8)  resize_reiserfs(8), debu
       greiserfs(8),

Reiserfsprogs-3.6.9         April 2003              REISERFSCK(8)
```

Page de manuel-de e2fsck

```
E2FSCK(8)                                                E2FSCK(8)


NAME
       e2fsck - check a Linux second extended file system

SYNOPSIS
       e2fsck  [ -pacnyrdfvstDFSV ] [ -b superblock ] [ -B block
```

size] [-l|-L bad_blocks_file] [-C fd] [-j external-journal] [-E extended_options] device

DESCRIPTION

e2fsck is used to check a Linux second extended file sys tem (ext2fs). E2fsck also supports ext2 filesystems coun taining a journal, which are also sometimes known as ext3 filesystems, by first applying the journal to the filesys tem before continuing with normal e2fsck processing. After the journal has been applied, a filesystem will nor mally be marked as clean. Hence, for ext3 filesystems, e2fsck will normally run the journal and exit, unless its superblock indicates that further checking is required.

device is the device file where the filesystem is stored (e.g. /dev/hdc1).

OPTIONS

-a This option does the same thing as the -p option. It is provided for backwards compatibility only; it is suggested that people use -p option whenever possible.

-b superblock
Instead of using the normal superblock, use an alternative superblock specified by superblock. This option is normally used when the primary superblock has been corrupted. The location of the backup superblock is dependent on the filesystem's blocksize. For filesystems with 1k blocksizes, a backup superblock can be found at block 8193; for filesystems with 2k blocksizes, at block 16384; and for 4k blocksizes, at block 32768.

Additional backup superblocks can be determined by using the mke2fs program using the -n option to print out where the superblocks were created. The -b option to mke2fs, which specifies blocksize of the filesystem must be specified in order for the superblock locations that are printed out to be accurate.

If an alternative superblock is specified and the

```
       filesystem is not  opened  read-only,  e2fsck  will
       make  sure  that  the primary superblock is updated
       appropriately upon  completion  of  the  filesystem
       check.

-B blocksize
       Normally,  e2fsck will search for the superblock at
       various different block sizes in an attempt to find
       the  appropriate  block  size.   This search can be
       fooled in some cases.  This option forces e2fsck to
       only  try  locating  the superblock at a particular
       blocksize.  If the superblock is not found,  e2fsck
       will terminate with a fatal error.

-c     This  option  causes e2fsck to run the badblocks(8)
       program to find any blocks which  are  bad  on  the
       filesystem,  and  then  marks them as bad by adding
       them to the bad block inode.   If  this  option  is
       specified  twice,  then  the bad block scan will be
       done using a non-destructive read-write test.

-C fd  This  option  causes  e2fsck  to  write  completion
       information  to  the  specified  file descriptor so
       that the progress of the filesystem  check  can  be
       monitored.   This  option is typically used by pro
       grams  which  are  running  e2fsck.   If  the  file
       descriptor specified is 0, e2fsck will print a com
       pletion bar as it goes about  its  business.   This
       requires  that e2fsck is running on a video console
       or terminal.

-d     Print debugging  output  (useless  unless  you  are
       debugging e2fsck).

-D     Optimize  directories  in  filesystem.  This option
       causes e2fsck to try to optimize  all  directories,
       either  by  reindexing  them if the filesystem sup
       ports directory indexing,  or by sorting  and  com
       pressing  directories  for  smaller directories, or
       for filesystems using traditional  linear  directo
       ries.

-E extended_options
```

Set e2fsck extended options. Extended options are comma separated, and may take an argument using the equals ('=') sign. The following options are supported:

ea_ver=extended_attribute_version
: Assume the format of the extended attribute blocks in the filesystem is the specified version number. The version number may be 1 or 2. The default extended attribute version format is 2.

-f
: Force checking even if the file system seems clean.

-F
: Flush the filesystem device's buffer caches before beginning. Only really useful for doing e2fsck time trials.

-j external-journal
: Set the pathname where the external-journal for this filesystem can be found.

-l filename
: Add the block numbers listed in the file specified by filename to the list of bad blocks. The format of this file is the same as the one generated by the badblocks(8) program. Note that the block numbers are based on the blocksize of the filesystem. Hence, badblocks(8) must be given the blocksize of the filesystem in order to obtain correct results. As a result, it is much simpler and safer to use the -c option to e2fsck, since it will assure that the correct parameters are passed to the badblocks program.

-L filename
: Set the bad blocks list to be the list of blocks specified by filename. (This option is the same as the -l option, except the bad blocks list is cleared before the blocks listed in the file are added to the bad blocks list.)

-n
: Open the filesystem read-only, and assume an answer

```
          of ‘no’ to all questions.  Allows e2fsck to be used
          non-interactively.   (Note:  if  the  -c, -l, or -L
          options are specified in addition to the -n option,
          then  the  filesystem will be opened read-write, to
          permit the bad-blocks list to be updated.  However,
          no other changes will be made to the filesystem.)

   -p     Automatically  repair  ("preen")  the  file  system
          without any questions.

   -r     This option does nothing at  all;  it  is  provided
          only for backwards compatibility.

   -s     This  option  will byte-swap the filesystem so that
          it is using  the  normalized,  standard  byte-order
          (which  is i386 or little endian).  If the filesys
          tem is already in the standard  byte-order,  e2fsck
          will take no action.

   -S     This  option will byte-swap the filesystem, regard
          less of its current byte-order.

   -t     Print timing statistics for e2fsck.  If this option
          is  used  twice,  additional  timing statistics are
          printed on a pass by pass basis.

   -v     Verbose mode.

   -V     Print version information and exit.

   -y     Assume an answer of ‘yes’ to all questions;  allows
          e2fsck to be used non-interactively.

EXIT CODE
   The exit code returned by e2fsck is the sum of the follow
   ing conditions:
        0    - No errors
        1    - File system errors corrected
        2    - File system errors corrected, system should
               be rebooted
        4    - File system errors left uncorrected
        8    - Operational error
        16   - Usage or syntax error
```

32   - E2fsck canceled by user request
128 - Shared library error

SIGNALS

The following signals have the following effect when sent to e2fsck.

SIGUSR1

This signal causes e2fsck to start displaying a completion bar. (See discussion of the -C option.)

SIGUSR2

This signal causes e2fsck to stop displaying a completion bar.

REPORTING BUGS

Almost any piece of software will have bugs. If you manage to find a filesystem which causes e2fsck to crash, or which e2fsck is unable to repair, please report it to the author.

Please include as much information as possible in your bug report. Ideally, include a complete transcript of the e2fsck run, so I can see exactly what error messages are displayed. If you have a writeable filesystem where the transcript can be stored, the script(1) program is a handy way to save the output of e2fsck to a file.

It is also useful to send the output of dumpe2fs(8). If a specific inode or inodes seems to be giving e2fsck trouble, try running the debugfs(8) command and send the output of the stat(1u) command run on the relevant inode(s). If the inode is a directory, the debugfs dump command will allow you to extract the contents of the directory inode, which can sent to me after being first run through uuencode(1).

Always include the full version string which e2fsck displays when it is run, so I know which version you are running.

AUTHOR

```
       This  version  of  e2fsck  was  written  by  Theodore Ts'o
       <tytso@mit.edu>.

SEE ALSO
       mke2fs(8), tune2fs(8), dumpe2fs(8), debugfs(8)

E2fsprogs version 1.34      July 2003                   E2FSCK(8)
```

Manual Page of xfs_check

```
xfs_check(8)                                            xfs_check(8)

NAME
       xfs_check - check XFS filesystem consistency

SYNOPSIS
  xfs_check [ -i ino ] ... [ -b bno ] ... [ -s ] [ -v ] xfs_special

  xfs_check -f [ -i ino ] ... [ -b bno ] ... [ -s ] [ -v ] file


DESCRIPTION
       xfs_check  checks  whether  an XFS filesystem is consistent.
       It is normally run only when there is reason to believe that
       the filesystem has a consistency problem.  The filesystem to
       be checked is specified by the xfs_special  argument,  which
       should  be  the  disk  or  volume device for the filesystem.
       Filesystems stored in files can also be checked,  using  the
       -f  flag.   The  filesystem  should normally be unmounted or
       read-only during the  execution  of  xfs_check.   Otherwise,
       spurious problems are reported.

       The options to xfs_check are:

       -f        Specifies  that  the  special  device is actually a
                 file (see the mkfs.xfs -d file option).  This might
                 happen  if  an  image copy of a filesystem has been
                 made into an ordinary file.

       -s        Specifies  that  only  serious  errors  should   be
                 reported.   Serious  errors  are those that make it
                 impossible to find major  data  structures  in  the
                 filesystem.   This  option  can be used to cut down
                 the amount of output when there is a serious  prob-
                 lem, when the output might make it difficult to see
                 what the real problem is.
```

-v Specifies verbose output; it is impossibly long for a reasonably-sized filesystem. This option is intended for internal use only.

-i ino Specifies verbose behavior for a specific inode. For instance, it can be used to locate all the blocks associated with a given inode.

-b bno Specifies verbose behavior for a specific filesystem block. For instance, it can be used to determine what a specific block is used for. The block number is a "file system block number". Conversion between disk addresses (i.e. addresses reported by xfs_bmap) and file system blocks may be accomplished using xfs_db's convert command.

Any non-verbose output from xfs_check means that the filesystem has an inconsistency. The filesystem can be repaired using either xfs_repair(8) to fix the filesystem in place, or by using xfsdump(8) and mkfs.xfs(8) to dump the filesystem, make a new filesystem, then use xfsrestore(8) to restore the data onto the new filesystem. Note that xfsdump may fail on a corrupt filesystem. However, if the filesystem is mountable, xfsdump can be used to try and save important data before repairing the filesystem with xfs_repair. If the filesystem is not mountable though, xfs_repair is the only viable option.

DIAGNOSTICS

Under one circumstance, xfs_check unfortunately might dump core rather than produce useful output. If the filesystem is completely corrupt, a core dump might be produced instead of the message xxx is not a valid filesystem

If the filesystem is very large (has many files) then xfs_check might run out of memory. In this case the message out of memory is printed.

The following is a description of the most likely problems and the associated messages. Most of the diagnostics produced are only meaningful with an understanding of the structure of the filesystem.

agf_freeblks n, counted m in ag a
    The freeblocks count in the allocation group header for allocation group a doesn't match the number of blocks counted free.

agf_longest n, counted m in ag a

The longest free extent in the allocation group header for allocation group a doesn't match the longest free extent found in the allocation group.

agi_count n, counted m in ag a
The allocated inode count in the allocation group header for allocation group a doesn't match the number of inodes counted in the allocation group.

agi_freecount n, counted m in ag a
The free inode count in the allocation group header for allocation group a doesn't match the number of inodes counted free in the allocation group.

block a/b expected inum 0 got i
The block number is specified as a pair (allocation group number, block in the allocation group). The block is used multiple times (shared), between multiple inodes. This message usually follows a message of the next type.

block a/b expected type unknown got y
The block is used multiple times (shared).

block a/b type unknown not expected
The block is unaccounted for (not in the freelist and not in use).

link count mismatch for inode nnn (name xxx), nlink m, counted n
The inode has a bad link count (number of references in directories).

rtblock b expected inum 0 got i
The block is used multiple times (shared), between multiple inodes. This message usually follows a message of the next type.

rtblock b expected type unknown got y
The real-time block is used multiple times (shared).

rtblock b type unknown not expected
The real-time block is unaccounted for (not in the freelist and not in use).

sb_fdblocks n, counted m
The number of free data blocks recorded in the superblock doesn't match the number counted free in the filesystem.

```
       sb_frextents n, counted m
              The number of free real-time extents recorded in  the
              superblock  doesn't  match the number counted free in
              the filesystem.

       sb_icount n, counted m
              The  number  of  allocated  inodes  recorded  in  the
              superblock  doesn't match the number allocated in the
              filesystem.

       sb_ifree n, counted m
              The number of free inodes recorded in the  superblock
              doesn't match the number free in the filesystem.

SEE ALSO
       mkfs.xfs(8),   xfsdump(8),   xfsrestore(8),   xfs_ncheck(8),
       xfs_repair(8), xfs(5).


                                                     xfs_check(8)
```

Manual Page of jfs_fsck

```
jfs_fsck(8)       JFS utility - file system check       jfs_fsck(8)

NAME
       jfs_fsck  -  initiate replay of the JFS transaction log, and
       check and repair a JFS formatted device


SYNOPSIS
       jfs_fsck [ -afnpvV ] [ -j journal_device  ]  [  --omit_jour-
       nal_replay ] [ --replay_journal_only ] device


DESCRIPTION
       jfs_fsck  is used to replay the JFS transaction log, check a
       JFS formatted device for errors, and fix any errors found.

       device is the special file name corresponding to the  actual
       device to be checked (e.g. /dev/hdb1).

       jfs_fsck must be run as root.

WARNING
       jfs_fsck should only be used to check an unmounted file sys-
       tem or a file system  that  is  mounted  READ  ONLY.   Using
```

```
       jfs_fsck to check a file system mounted other than READ ONLY
       could seriously damage the file system!

OPTIONS
       If no options are selected, the default is -p.

       -a     Autocheck mode - Replay the transaction log.  Do  not
              continue  fsck  processing unless the aggregate state
              is dirty or  the  log  replay  failed.   Functionally
              equivalent  to  -p.   Autocheck mode is typically the
              default mode used when jfs_fsck  is  called  at  boot
              time.

       -f     Replay the transaction log and force checking even if
              the file system appears clean.  Repair  all  problems
              automatically.

       -j journal_device
              Specify the journal device.

       -n     Open  the  file  system read only.  Do not replay the
              transaction log.  Report errors, but  do  not  repair
              them.

       --omit_journal_replay
              Omit  the replay of the transaction log.  This option
              should not be used unless as a last resort (i.e.  the
              log  has  been  severely  corrupted  and replaying it
              causes further problems).

       -p     Automatically  repair  ("preen")  the  file   system.
              Replay  the  transaction  log.   Do not continue fsck
              processing unless the aggregate state is dirty or the
              log replay failed.  Functionally equivalent to -a.

       --replay_journal_only
              Only  replay  the  transaction  log.  Do not continue
              with a full file system check if the replay fails  or
              if  the file system is still dirty even after a jour-
              nal replay.  In general, this option should  only  be
              used  for  debugging  purposes  as it could leave the
              file system in an  unmountable  state.   This  option
              cannot be used with -f, -n, or --omit_journal_replay.

       -v     Verbose messaging - print details  and  debug  state-
              ments to stdout.

       -V     Print version information and exit (regardless of any
              other chosen options).
```

EXAMPLES

Check the 3rd partition on the 2nd hard disk, print extended information to stdout, replay the transaction log, force complete jfs_fsck checking, and give permission to repair all errors:

```
jfs_fsck -v -f /dev/hdb3
```

Check the 5th partition on the 1st hard disk, and report, but do not repair, any errors:

```
jfs_fsck -n /dev/hda5
```

EXIT CODE

The exit code returned by jfs_fsck represents one of the following conditions:

0 No errors

1 File system errors corrected and/or transaction log replayed successfully

2 File system errors corrected, system should be rebooted if file system was mounted

4 File system errors left uncorrected

8 Operational error

16 Usage or syntax error

128 Shared library error

REPORTING BUGS

If you find a bug in JFS or jfs_fsck, please report it via the bug tracking system ("Report Bugs" section) of the JFS project web site:
http://oss.software.ibm.com/jfs

Please send as much pertinent information as possible, including the complete output of running jfs_fsck with the -v option on the JFS device.

SEE ALSO

fsck(8), jfs_mkfs(8), jfs_fscklog(8), jfs_tune(8), jfs_logdump(8), jfs_debugfs(8)

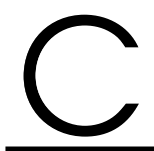
AUTHORS

Barry Arndt (barndt@us.ibm.com)

```
William Braswell, Jr.

jfs_fsck is maintained by IBM.
See the JFS project web site for more details:
http://oss.software.ibm.com/jfs

                   October 29, 2002              jfs_fsck(8)
```



The GNU General Public License

GNU General Public License

Foreword

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the *GNU General Public License* is intended to guarantee your freedom to share and change free software — to make sure the software is free for all its users. This *General Public License* applies to most of the *Free Software Foundation's* software and to any other program whose authors commit to using it. (Some other *Free Software Foundation* software is covered by the *GNU Library General Public License* instead.) You can apply it to your programs, too.

When we speak of *"free" software*, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you

receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

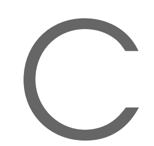
Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU General, Public License

Terms and Conditions for Copying, Distribution and Modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this *General Public License*. The "Program", below, refers to any such program or work, and a *work based on the Program* means either the Program or any derivative work



under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term ”modification“.) Each licensee is addressed as ”you“.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

1. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
2. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
3. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

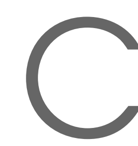
Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

1. Accompany it with the complete corresponding machine--readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
2. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
3. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, "complete source code" means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on



which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty--free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

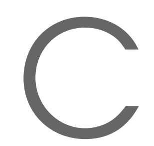
9. The *Free Software Foundation* may publish revised and/or new versions of the *General Public License* from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the *Free Software Foundation*. If the Program does not specify a version number of this License, you may choose any version ever published by the *Free Software Foundation*.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the *Free Software Foundation*, write to the *Free Software Foundation*; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

No Warranty

11. Because the program is licensed free of charge, there is no warranty for the program, to the extent permitted by applicable law. Except when otherwise stated in writing the copyright holders and/or other parties provide the program



"as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the program is with you. Should the program prove defective, you assume the cost of all necessary servicing, repair or correction.

12. In no event unless required by applicable law or agreed to in writing will any copyright holder, or any other party who may modify and/or redistribute the program as permitted above, be liable to you for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use the program (including but not limited to loss of data or data being rendered inaccurate or losses sustained by you or third parties or a failure of the program to operate with any other programs), even if such holder or other party has been advised of the possibility of such damages.

End of Terms and Conditions

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
<one line to give the program’s name and a brief
idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.
```

```
You should have received a copy of the GNU General Public
License along with this program; if not, write to the Free
Software Foundation, Inc., 59 Temple Place, Suite 330, Boston,
MA 02111-1307, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) <year> <name of author>

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type
'show w'. This is free software, and you  are welcome to
redistribute it under certain conditions; type 'show c' for
details.
```

The hypothetical commands `show w` and `show c` should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w` and `show c`; they could even be mouse-clicks or menu items—whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the
program 'Gnomovision' (which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1st April 1989 Ty Coon, President of Vice
```

This *General Public License* does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the *GNU Library General Public License* instead of this License.

Glossaire

ACL (Access Control List)
Extension du concept traditionnel de droits sur les fichiers et les répertoires. Elles permettent une gestion plus fine des droits d'accès.

Administrateur système (system administrator)
Voir root.

Adresse IP (IP address)
Adresse numérique unique sur 32 bits d'un ordinateur au sein d'un réseau TCP/IP. On l'écrit souvent sous la forme de quatre nombres décimaux séparés par des points (par exemple 192.168.10.1).

ADSL (Asymmetric Digital Subscriber Line)
Protocole rapide de transfert de données s'appuyant sur le réseau téléphonique.

AGP (Accelerated Graphics Port)
Connecteur rapide pour cartes graphiques qui offre une meilleure bande passante que celle des connecteurs PCI. Les cartes graphiques AGP peuvent accéder directement (sans passer par le processeur) à la mémoire centrale.

Amorçage (booting)
La suite d'opérations accomplies par l'ordinateur depuis l'allumage de la machine jusqu'au moment où le système est prêt à être utilisé.

ATAPI (Advance Technology Attachment Packet Interface)
ATAPI est un type de lecteur de CD-ROM connecté à un contrôleur IDE ou EIDE. À côté des lecteurs ATAPI, il existe des lecteurs de CD-ROM SCSI qui sont gérés par un contrôleur SCSI.

Bande passante (bandwidth)

Débit maximal d'un canal de transmission de données. Ce terme est en général utilisé pour les connexions réseau.

BIOS (Basic Input-Output System)

Petit programme qui est lancé après l'allumage ou le redémarrage d'un ordinateur. Il se charge de l'initialisation des composants matériels. La plupart des BIOS permettent de modifier les options de bas niveau du système au moyen d'un programme de paramétrage interactif. Le code de ce programme réside sur une puce de mémoire morte (ROM).

Chemin d'accès (path)

Le chemin d'accès définit sans aucune ambiguïté l'emplacement d'un fichier à l'intérieur d'un système de fichiers.

Client (client)

Un programme ou un ordinateur au sein d'un réseau qui se connecte à un serveur et lui demande des informations.

Compte (account)

Le compte est l'ensemble constitué par le nom d'utilisateur et le mot de passe. Un compte correspond à un identifiant utilisateur (UID, user identifier).

Connexion (login)

Procédure d'authentification d'un utilisateur au moyen d'un nom d'utilisateur et d'un mot de passe lui permettant d'accéder à un système informatique ou à un réseau.

Console (console)

Autrefois, la console était synonyme de terminal. Sous Linux les *consoles virtuelles* permettent d'utiliser un seul écran pour plusieurs sessions de travail indépendantes mais simultanées.

Courrier électronique (e-mail)

Méthode de transport électronique du courrier entre utilisateurs au travers d'un réseau. Une adresse de courrier électronique est de la forme `nom_utilisateur@domaine.org`.

CPU (Central Processing Unit)

Voir Processeur.

Curseur (cursor)
Le curseur est un petit bloc ou caractère de soulignement qui marque l'emplacement où l'on saisit du texte.

DDC (Direct Display Channel)
Standard de communication entre le moniteur et la carte graphique qui permet de passer certains paramètres tels que le nom du moniteur ou la résolution.

Déconnexion (logout)
Procédure consistant à fermer une session Linux interactive.

Démon (daemon)
Un démon (de l'anglais daemon, Disk And Execution MONitor) est un programme qui veille en arrière-plan et entre en action en cas de besoin. Le démon HTTP répond par exemple aux requêtes HTTP.

DNS (Domain Name System)
Un protocole qui permet de convertir des noms d'hôtes en adresses IP et vice-versa.

Droits d'accès (access permissions)
Les droits d'accès à un fichier déterminent si un utilisateur ou un groupe peuvent lire, écrire ou exécuter un fichier ou un répertoire. Ils sont généralement réglés par l'administrateur système.

EIDE (Enhanced Integrated Drive Electronics)
Standard IDE amélioré qui permet d'utiliser des disques durs de plus de 512 Mo.

Environnement (environment)
L'ensemble des variables d'environnement et de leurs valeurs manipulées par l'interpréteur de commandes. L'utilisateur peut modifier ou retirer l'affectation de variables existantes et affecter des valeurs à de nouvelles variables. On peut leur affecter des valeurs de façon permanente au moyen des fichiers de configuration de l'interpréteur de commandes.

Ethernet
Un standard pour transporter des données dans un réseau d'ordinateurs.

EXT2 (Second Extended File System)
Un système de fichiers pris en charge par Linux.

FAQ (Foire Aux Questions)
Acronyme désignant les documents qui donnent des réponses aux questions fréquemment posées.

FTP (File Transfer Protocol)
Un protocole basé sur TCP/IP pour le transfert de fichiers en réseau.

Gestionnaire de fenêtres (window manager)
Un programme qui fonctionne en s'appuyant sur le système X Window et qui permet par exemple de changer la taille des fenêtres et de les déplacer. Le gestionnaire de fenêtres se charge également des décorations des fenêtres comme la barre de titres et les bords. Le comportement et l'apparence peuvent être ajustés par l'utilisateur.

GNOME (GNU Network Object Model Environment)
Un environnement de bureau graphique pour Linux.

GNU (GNU is Not Unix)
GNU est un projet de la Free Software Foundation (FSF). L'objectif du projet GNU est de créer un système d'exploitation complet et libre de type UNIX. Le mot anglais "free" n'est pas tant employé ici dans le sens de *gratuit* que celui de *libre* : avoir le droit d'obtenir, de modifier et de redistribuer les logiciels. Le désormais classique manifeste GNU (`http://www.gnu.org/gnu/manifesto.html`) donne les détails. D'un point de vue juridique, les logiciels GNU sont protégés par la GNU General Public License, en abrégé GPL (`http://www.gnu.org/copyleft/gpl.html`), ou par la GNU Lesser General Public License, en abrégé LGPL (`http://www.gnu.org/copyleft/lgpl.html`). Le noyau Linux, qui est soumis à la GPL, profite du projet GNU, en particulier en ce qui concerne les utilitaires, mais ne doit pas être confondu avec lui.

GPL (GNU General Public License)
Voir GNU.

HTML (Hypertext Markup Language)
Un langage de balisage de documents de texte utilisé sur le Web (World Wide Web). Les documents HTML sont la plupart du temps consultés au moyen d'un navigateur.

HTTP (Hypertext Transfer Protocol)
Un protocole réseau qui définit comment demander et transférer des documents sur le Web (World Wide Web). Ces documents sont en général des pages HTML offertes par un serveur et demandées par un utilisateur depuis son navigateur.

IDE (Integrated Drive Electronics)
Un standard permettant de connecter des disques durs.

Internet
Réseau mondial basé sur le protocole TCP/IP.

Interpréteur de commandes (shell)
Un programme interactif qui permet de soumettre des commandes. Il existe différent types d'interpréteurs de commandes dont bash, zsh et tcsh. Chaque type d'interpréteur de commandes dispose de son propre langage de programmation.

Invite (prompt)
Une chaîne de caractères courte et pouvant être configurée qui s'affiche au début de chaque commande. Elle contient d'habitude le répertoire courant.

IRQ (Interrupt Request)
Une demande asynchrone d'accomplir une certaine action. Cette demande peut être déclenchée par un programme ou un composant matériel. La plupart des IRQ sont traitées par le système d'exploitation.

Joker (wild card)
Caractère de substitution représentant un caractère (symbole : ?) ou plusieurs caractères (symbole : *). De tels caractères sont utilisés dans les expression régulières, également appelées expression rationnelles.

KDE (K Desktop Environment)
Un environnement de bureau graphique pour Linux.

Lien (link)
Un lien (au sein d'un système de fichiers) est un pointeur vers un fichier. Il existe des liens *en dur* et des liens *symboliques*. Tandis que les liens *en dur* font référence à un emplacement précis du système de fichiers, les liens *symboliques* ne font référence qu'au nom du fichier.

Ligne de commande (command line)

Façon de soumettre des commandes à un ordinateur basée sur le mode texte.

LILO (Linux Loader)

Petit programme installé dans le secteur d'amorçage du disque dur et qui peut lancer aussi bien Linux que d'autres systèmes d'exploitation.

Linux

Partie centrale d'un système d'exploitation de type UNIX, librement distribué selon les termes de la licence GPL (GNU). Son nom (*Linus' uniX*) dérive du nom de son créateur, Linus Torvalds. Bien que ce terme ne s'applique à proprement parler qu'au noyau, on entend généralement par *Linux* l'ensemble du système d'exploitation.

MD5

Un algorithme pour générer des sommes de contrôle d'un fichier. Ces sommes sont générées de telle façon qu'il est pratiquement impossible de créer un fichier qui a une somme MD5 identique mais un contenu différent de celui du fichier de départ.

Mémoire centrale (main memory)

Mémoire physique de capacité limitée à laquelle on peut accéder rapidement. On la désigne souvent sous le nom de mémoire vive (RAM, Random Access Memory).

Montage (mounting)

Procédé qui consiste à rattacher un système de fichiers à l'arborescence des répertoires du système.

MP3

Procédé de compression très efficace pour des fichiers audio. La taille d'un fichier compressé est à peu près dix fois plus petite que la taille du même fichier audio non compressé.

Multi-utilisateurs (multiuser)

Un système multi-utilisateurs est un système d'exploitation qui permet à plusieurs personnes de travailler simultanément sur un même ordinateur.

Multitâche (multitasking)

Les systèmes d'exploitation qui peuvent exécuter presque simultanément plusieurs processus sont appelés systèmes multitâches.

Navigateur (browser)
Programme qui affiche le contenu de fichiers locaux ou de pages web.

NFS (Network File System)
Un protocole pour accéder à un système de fichiers en réseau.

NIS (Network Information Service)
Système en réseau pour la gestion centrale des informations d'administration des utilisateurs. NIS permet de gérer les noms d'utilisateurs et les mots de passe sur l'ensemble du réseau.

Nom d'hôte (hostname)
Nom d'une machine. Il s'agit souvent du nom sous lequel on peut y accéder dans le réseau.

Noyau (kernel)
Le noyau est le cœur du système d'exploitation. Il gère la mémoire et les systèmes de fichiers, il contient les pilotes qui se chargent de communiquer avec les périphériques et il gère les processus et le réseau.

Pages de manuel (man pages)
La documentation des systèmes Unix se trouve traditionnellement dans les pages de manuel (man pages) que l'on peut consulter avec la commande `man`. Les pages de manuel sont le plus souvent écrites comme des textes de référence.

Pare-feu (firewall)
Un mécanisme qui permet de filtrer le trafic réseau afin d'empêcher d'accéder sans autorisation au réseau local depuis l'extérieur.

Partition (partition)
Une section d'un disque dur qui contiennent soit un système de fichiers soit un espace d'échange.

Pilote (driver)
Composant du système d'exploitation dont le rôle est de communiquer avec les composants matériels.

Plug and Play
Protocole de détection et de configuration automatique du matériel.

Processeur (processor)
Le processeur (CPU, Central Processing Unit) est un circuit intégré qui exécute le code machine qui réside en mémoire centrale. Il s'agit du *cerveau* de l'ordinateur.

Processus (process)
Un programme en cours d'exécution. On les désigne parfois sous le nom de tâches.

Protocole (protocol)
Un standard qui définit les interfaces et les méthodes de communication au niveau matériel et logiciel, ainsi qu'au niveau du réseau. HTTP et FTP sont des exemples de protocoles.

RAM (Random Access Memory)
Voir Mémoire centrale.

ReiserFS
Un système de fichiers qui permet de réparer rapidement d'éventuelles incohérences. De telles incohérences peuvent se produire lorsqu'un système de fichiers n'est pas démonté avant l'arrêt du système, par exemple en cas de panne de courant.

Répertoire (directory)
Une structure qui contient des fichiers ou d'autres répertoires (les sous-répertoires). Les répertoires forment une structure arborescente qui permet d'organiser les fichiers.

Répertoire personnel (home directory)
Répertoire privé dans le système de fichiers qui appartient à un utilisateur donné (généralement `/home/<nom_utilisateur>`). Cet utilisateur est le seul avec le super-utilisateur à avoir tous les droits sur ce répertoire.

Répertoire racine (root directory)
Le répertoire situé au à la base de la hiérarchie des fichiers du système de fichiers. Sous UNIX, le répertoire racine est symbolisé par `/`.

Répertoire utilisateur (user directory)
Voir Répertoire personnel.

Réseau (network)
: Une interconnexion de plusieurs ordinateurs qui permet de transférer des données de l'un à l'autre. Un ordinateur qui envoie une requête en réseau est souvent désigné sous le nom de client, tandis que l'ordinateur qui répond à la requête (par exemple en renvoyant un document) est appelé serveur.

Réseau local (LAN, Local Area Network)
: Réseau informatique s'étendant sur un rayon très limité.

RNIS (ISDN, Integrated Services Digital Network)
: Un standard pour le transfert de données numériques à travers un réseau téléphonique.

root
: Le compte du super-utilisateur. Il a tous les droits. Ce compte est utilisé pour les tâches administratives et ne devrait pas être employé pour le travail courant.

Sauvegarde (backup)
: Une sauvegarde est une copie de données utilisée pour récupérer des données qui ont été endommagées ou perdues. On devrait faire régulièrement des sauvegardes de toutes les données importantes.

SCSI (Small Computer Systems Interface)
: Un standard pour connecter des disques durs et d'autres périphériques tels que des scanneurs et des unités de bandes.

Secteur d'amorçage maître (MBR, Master Boot Record)
: Le premier secteur physique d'un disque dur dont le contenu est chargé en mémoire centrale puis exécuté par le BIOS. Ce code charge soit le système d'exploitation à partir d'une partition de disque dur amorçable, soit un chargeur d'amorçage plus évolué tel que LILO ou GRUB.

Serveur (server)
: Un ordinateur ou un programme spécialisé afin d'offrir des services, généralement en réseau. HTTP, DNS et FTP sont des exemples de types de services.

Serveur mandataire (proxy)
: Il s'agit en général d'un ordinateur qui sert d'espace de stockage intermédiaire pour les données provenant de l'Internet. Si un même document

est demandé plusieurs fois, il sera remis beaucoup plus rapidement à partir de la deuxième requête. Les ordinateurs qui sont censés en tirer avantage doivent être configurés de manière à émettre leurs requêtes par le truchement du serveur mandataire.

Signet (bookmark)
Une URL au sein d'une collection de telles adresses.

SMTP (Simple Mail Transfer Protocol)
Protocole permettant d'acheminer du courrier électronique en réseau.

SSL (Secure Socket Layer)
Protocole de chiffrement permettant de transférer des données HTTP.

Super-utilisateur (super user)
Voir root.

Système d'exploitation (operating system)
Voir Noyau.

Système X Window (X Window System)
Le système X Window est une interface graphique en réseau qui fonctionne sur une vaste gamme d'ordinateurs. Il offre des primitives permettant de tracer des lignes ou des rectangles. Il s'agit d'une couche intermédiaire entre le matériel et le gestionnaire de fenêtres.

Tâche (task)
Voir Processus.

TCP/IP
Protocole de communication utilisé sur l'Internet, ainsi que sur la plupart des réseaux locaux.

Telnet
Telnet est un protocole et la commande permettant de communiquer avec des machines distantes. Pour se connecter à distance, Telnet est à présent remplacé par SSH qui offre le chiffrement des connexions.

Terminal (terminal)
Ce terme désignait autrefois l'association d'un clavier et d'un écran reliée à un ordinateur central. De nos jours, ce terme est plutôt utilisé pour des programmes (comme xterm) qui émulent un vrai terminal.

Tux
: Nom du manchot mascotte de Linux (voir `http://www.sjbaker.org/tux/`) souvent qualifié de "pingouin" par erreur de traduction de l'anglais "penguin".

UNIX
: UNIX est une marque déposée et un type de systèmes d'exploitation.

URL (Uniform Resource Locator)
: Indication d'une ressource du réseau composée d'un protocole (par exemple `http://`), du nom du serveur et du domaine (par exemple `www.suse.de`) et du nom d'un document (par exemple `/us/company/index.html`, ce qui donne par exemple `http://www.suse.de/us/company/index.html`.

Variable d'environnement (environment variable)
: Un élément de l'environnement de l'interpréteur de commandes.

VESA (Video Electronics Standard Association)
: Consortium industriel qui définit, entre autres, des standards vidéo.

WWW (World Wide Web)
: Partie graphique de l'Internet basée sur le protocole HTTP et que l'on peut parcourir avec un navigateur web.

X11
: Version 11 du Système X Window.

YaST (Yet another Setup Tool)
: L'assistant système de SUSE LINUX.

YP (yellow pages)
: Voir NIS.

Index

Symboles

B

C

D

E

F

G

H

I

J

K

L

Z